Sol P0372 US00
#4

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年 ３月１４日

出願番号
Application Number: 特願２０００－０６９７８８

出願人
Applicant (s): ソニー株式会社

２００１年 １月 ５日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３１０９４６０

【書類名】　特許願

【整理番号】　99009861

【提出日】　平成12年 3月14日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/60

【発明の名称】　コンテンツ取り引きシステムおよびコンテンツ取り引き方法、並びにプログラム提供媒体

【請求項の数】　27

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　石橋　義人

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　松山　科子

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　渡辺　秀明

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　二村　一郎

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　昆　雅士

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　062721

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ取り引きシステムおよびコンテンツ取り引き方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項１】

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引きシステムにおいて、

前記ユーザデバイスは、クリアリングセンタの発行した発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行する構成を有し、

サービスプロバイダは、前記ユーザデバイスから受信する前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成してクリアリングセンタに送信する処理を実行する構成を有し、

クリアリングセンタは、前記サービスプロバイダから受信する前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するとともに、利用料振替処理要求を口座管理機関に送信する処理を実行する構成を有し、

口座管理機関は、前記振替処理要求に従った口座間の振替処理を実行する構成を有することを特徴とするコンテンツ取り引きシステム。

【請求項２】

前記ユーザデバイスと前記サービスプロバイダは各々暗号処理部を有し、

前記ユーザデバイスから前記サービスプロバイダへの利用ログ送信の際は、前記ユーザデバイスと前記サービスプロバイダ間において相互認証処理を実行し、さらに、前記ユーザデバイスは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記サービスプロバイダは該電子署名の検証処理を実行する構成であることを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項３】

前記サービスプロバイダと前記クリアリングセンタは各々暗号処理部を有し、

前記サービスプロバイダから前記クリアリングセンタへの受領ログ送信の際は、前記サービスプロバイダと前記クリアリングセンタ間において相互認証処理を実行し、さらに、前記サービスプロバイダは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記クリアリングセンタは該電子署名の検証処理を実行する構成であることを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項４】

前記クリアリングセンタは、前記ユーザデバイスの電子マネー残高を管理するユーザ残高データベースを有し、該ユーザ残高データベースに登録された電子マネー残高に応じて前記発行ログを生成して前記ユーザデバイスに送信する構成を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項５】

前記クリアリングセンタと前記ユーザデバイスとは各々暗号処理部を有し、

前記クリアリングセンタから前記ユーザデバイスへの発行ログ送信の際は、前記クリアリングセンタと前記ユーザデバイス間において相互認証処理を実行し、さらに、前記クリアリングセンタは、前記発行ログに対して電子署名の生成処理を実行して、前記発行ログを受信した前記ユーザデバイスは該電子署名の検証処理を実行する構成であることを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項６】

前記販売条件情報は、

前記ユーザデバイスによるコンテンツ利用料の配分情報を含み、

前記利用ログおよび前記受領ログは前記配分情報を含んで構成され、前記クリアリングセンタは、前記配分情報に基づいてコンテンツ利用料の電子マネーに関する精算処理を実行するとともに、前記振替要求の前記口座管理機関に対する送信処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項７】

前記ユーザデバイスに提供されるコンテンツは、暗号化コンテンツと前記販売条件を含むデータにコンテンツ提供者の電子署名がなされたセキュアコンテナ構成を有し、

前記ユーザデバイスは前記セキュアコンテナの電子署名の検証を実行して前記セキコンテナの改竄の有無について判定する構成を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項８】

前記ユーザデバイス、前記サービスプロバイダ、前記クリアリングセンタいずれか相互間におけるログデータの送受信は、公開鍵証明書発行局の発行したデータ送信側の公開鍵証明書を添付して実行する構成であることを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項９】

前記発行ログは、ユーザデバイス識別子またはユーザ識別子の少なくともいずれかの識別子、および電子マネーによる支払可能な発行金額データを含む発行情報を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１０】

前記利用ログは、前記発行ログを含み、さらに、コンテンツの利用金額と、利用金額の受け取り先データとを含む利用情報を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１１】

前記受領ログは、前記利用ログを含み、さらに、コンテンツの利用金額支払元データを含む受領情報を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１２】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行する構成であり、

前記クリアリングセンタは、前記口座管理機関にあるクリアリングセンタ管理口座に前記ユーザデバイスのユーザからの振り込み済みの金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信する構成を有するこ

とを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１３】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行する構成であり、

前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合、前記ユーザデバイスに対して該ユーザデバイスの電子マネー残高情報を要求し、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信する構成を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１４】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行する構成であり、

前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合において、前記ユーザデバイスから受領した該ユーザデバイスの電子マネー残高情報に基づいて、発行済みの発行ログに基づく支払い処理の未回収分の存在が判明した場合、シリアル番号の異なる新たな発行ログを、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定して前記ユーザデバイスに対して送信する構成を有することを特徴とする請求項１に記載のコンテンツ取り引きシステム。

【請求項１５】

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き方法において、

前記ユーザデバイスは、クリアリングセンタの発行した発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行し、

サービスプロバイダは、前記ユーザデバイスから受信する前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成してクリアリングセンタに送信する処理を実行し、

クリアリングセンタは、前記サービスプロバイダから受信する前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するとともに、利用料振替処理要求を口座管理機関に送信する処理を実行し、

口座管理機関は、前記振替処理要求に従った口座間の振替処理を実行することを特徴とするコンテンツ取り引き方法。

【請求項１６】

前記ユーザデバイスと前記サービスプロバイダは各々暗号処理部を有し、

前記ユーザデバイスから前記サービスプロバイダへの利用ログ送信の際は、前記ユーザデバイスと前記サービスプロバイダ間において相互認証処理を実行し、

前記ユーザデバイスは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記サービスプロバイダは該電子署名の検証処理を実行することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項１７】

前記サービスプロバイダと前記クリアリングセンタは各々暗号処理部を有し、

前記サービスプロバイダから前記クリアリングセンタへの受領ログ送信の際は、前記サービスプロバイダと前記クリアリングセンタ間において相互認証処理を実行し、

前記サービスプロバイダは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記クリアリングセンタは該電子署名の検証処理を実行することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項１８】

前記クリアリングセンタは、前記ユーザデバイスの電子マネー残高を管理するユーザ残高データベースを有し、該ユーザ残高データベースに登録された電子マネー残高に応じて前記発行ログを生成して前記ユーザデバイスに送信することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項１９】

前記クリアリングセンタと前記ユーザデバイスとは各々暗号処理部を有し、

前記クリアリングセンタから前記ユーザデバイスへの発行ログ送信の際は、前記クリアリングセンタと前記ユーザデバイス間において相互認証処理を実行し、

前記クリアリングセンタは、前記発行ログに対して電子署名の生成処理を実行して、前記発行ログを受信した前記ユーザデバイスは該電子署名の検証処理を実行することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２０】

前記販売条件情報は、

前記ユーザデバイスによるコンテンツ利用料の配分情報を含み、前記利用ログおよび前記受領ログは前記配分情報を含んで構成され、

前記クリアリングセンタは、前記配分情報に基づいてコンテンツ利用料の電子マネーに関する精算処理を実行するとともに、前記振替要求の前記口座管理機関に対する送信処理を実行することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２１】

前記ユーザデバイスに提供されるコンテンツは、暗号化コンテンツと前記販売条件を含むデータにコンテンツ提供者の電子署名がなされたセキュアコンテナ構成を有し、

前記ユーザデバイスは前記セキュアコンテナの電子署名の検証を実行して前記セキコンテナの改竄の有無について判定することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２２】

前記ユーザデバイス、前記サービスプロバイダ、前記クリアリングセンタいずれか相互間におけるログデータの送受信は、公開鍵証明書発行局の発行したデータ送信側の公開鍵証明書を添付して実行することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２３】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、

前記クリアリングセンタは、前記口座管理機関にあるクリアリングセンタ管理口座に前記ユーザデバイスのユーザからの振り込み済みの金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２４】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、

前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合、前記ユーザデバイスに対して該ユーザデバイスの電子マネー残高情報を要求し、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２５】

前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、

前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合において、前記ユーザデバイスから受領した該ユーザデバイスの電子マネー残高情報に基づいて、発行済みの発行ログに基づく支払い処理の未回収分の存在が判明した場合、シリアル番号の異なる新たな発行ログを、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定して前記ユーザデバイスに対して送信することを特徴とする請求項１５に記載のコンテンツ取り引き方法。

【請求項２６】

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プ

ログラムは、

発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行するステップを有することを特徴とするプログラム提供媒体。

【請求項２７】

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

発行ログに設定された発行金額を限度として、コンテンツの利用金額データを含むコンテンツ利用ログを生成するステップ、

前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成するステップと、

前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するステップと、

を協動的に実行することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンテンツ取り引きシステムおよびコンテンツ取り引き方法、並びにプログラム提供媒体に関する。特に、音楽、画像データ、ゲームプログラム等の各種コンテンツ情報をＣＤ，ＤＶＤ等の記録媒体を介して、あるいはネットワークを介した配信によりユーザに提供し、ユーザからコンテンツ利用に伴う利用料金の回収あるいは利用ポイントの付与等を実行する構成を有するコンテンツ取り引きシステムおよびコンテンツ取り引き方法に関する。

【０００２】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、

様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはＤＶＤ、ＣＤ等の流通可能な記憶媒体（メディア）を介して流通している。これらの流通コンテンツは、一般にユーザの所有するＰＣ（Personal Computer）、ゲーム機器等の記録再生機器において再生し、また付属する記録デバイス、例えばＥＥＰＲＯＭ、フラッシュメモリ等によって構成されるメモリカード、ハードディスク等に格納することが可能である。

【０００３】

ＤＶＤ、ＣＤ等の流通可能な記憶媒体（メディア）、あるいはメモリカード等の記憶手段に記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により各記憶手段から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００４】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、コンテンツの配布時、すなわちコンテンツがネットワークを介して、あるいはＤＶＤ，ＣＤ等の記憶媒体によって流通する場合には、コンテンツの提供時に代金を回収したり、インターネット等のネットワークを介してコンテンツを配信する場合、コンテンツ配信に際してユーザのクレジット番号等のユーザ情報を取得してユーザからコンテンツ提供に対する対価、すなわち利用料金を取得する構成を採用している。

【０００５】

これらのコンテンツの配布に際しては、コンテンツの許可のない複製等が行われないよう、セキュリティを考慮した構成をとるのが一般的となっており、ＤＶＤ，ＣＤ等の記憶媒体（メディア）、あるいはネットワークを介したコンテンツデータの配信においては、配布コンテンツを正規なユーザに対してのみ提供する構成が各種提案されている。

【０００６】

コンテンツ利用を正規ユーザにのみ提供する概念の１つに「超流通」という考えが提案されている。「超流通」は、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータであるコンテンツの提供者、あるいはコンテンツ管理者の権利保護を確保して、コンテンツを流通させるための構成である。この「超流通」の構成を図1に示す。

【０００７】

コンテンツプロバイダ１０１、コンテンツプロバイダ１０２は、それぞれコンテンツ１０３，１０４をユーザ端末１０５に提供する。コンテンツ１０３、１０４には、コンテンツ固有の識別子であるコンテンツＩＤが付加されている。ユーザ端末１０５では、コンテンツＩＤの付加されたコンテンツを受領すると、判定処理部１０７において、ユーザ端末１０５が、そのコンテンツの利用可能な正規ユーザ端末であるか否かを判定する。この判定処理は、記憶部１，１０６に記憶されたユーザ端末のユーザＩＤとコンテンツ利用条件に基づいて判定される。コンテンツ利用条件は、ユーザ毎にコンテンツプロバイダが予め設定したコンテンツの利用条件である。設定したコンテンツ利用条件に応じてコンテンツの利用可と判定されると、そのコンテンツの利用履歴を記憶部２，１０８にユーザＩＤとコンテンツＩＤを対応させて記憶する。

【０００８】

コンテンツプロバイダ１０１，１０２は、ユーザ端末１０５の記憶部２，１０８に記憶されたコンテンツ利用履歴を回収して、その履歴に従ってコンテンツ利用料金をユーザに請求することができる。このように「超流通」は、ユーザ毎にコンテンツの利用条件を判定し、かつコンテンツ毎に利用履歴を記録する構成により、コンテンツの利用を正規ユーザに限定し、利用料金の回収を可能にする構成である。

【０００９】

しかしながら、上記の「超流通」の構成はコンテンツの利用履歴を記録する構成を開示しているものの、利用履歴に基づく料金徴収システムについては明確に示すものではなく、料金の支払い手法は従来から提案されている方法を採用する

ことになる。例えば（１）クレジットカード番号をユーザ端末から入力してコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツの利用権を管理するコンテンツ利用権販売センタに送信する。（２）ユーザの銀行口座番号を端末から入力してコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタに送信する。（３）予めコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタにユーザ登録を行ない、クレジットカード番号、あるいは銀行口座番号を登録し、コンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタが登録済みデータに基づいて料金引き落としを実行する。これらのいずれかの方法を実行することが必要となる。

【００１０】

上述の（１）～（３）の支払方法においてはユーザのクレジットカード番号、あるいは銀行口座番号が要求されることになる。従って、これらのクレジットカード、銀行口座を持たない者にとっては、この支払い手続きが困難になる。さらに、昨今では、取り引きコンテンツ単位が小口化し、例えば音楽コンテンツの配信において曲目１曲のみを取り引きコンテンツとすることもある。このような場合、コンテンツの代金は、１００円単位、１０００円単位の小額のものとなり、これらの支払いにおいて、逐一、クレジットカード番号、あるいは銀行口座番号が要求されるという取り引き形態がコンテンツの流通を妨げる一因ともなっている。

【００１１】

さらに、一旦市場に流通したコンテンツは、さらにユーザ間において取り引き、譲渡され得る。このようなユーザ間での取り引きを管理することは困難であり、不正なコピーの流通が氾濫することになる。また、ユーザ間の取り引きにおいては、一般にコンテンツを提供したユーザに対して何ら保証されないのが一般的であった。

【００１２】

【発明が解決しようとする課題】

本発明は、これらの状況に鑑みてなされたものであり、ゲームプログラム、音

楽データ、画像データ等、多くのソフトウエア・コンテンツ利用権の販売において、クレジットカード番号、あるいは銀行口座番号を利用せず、簡易な方法、構成のコンテンツ取り引きを可能として、ユーザ間の取り引き管理、精算処理等も可能とするコンテンツ取り引きシステムおよびコンテンツ取り引き方法、並びにプログラム提供媒体を提供することを目的とする。

【００１３】

【課題を解決するための手段】

本発明の第１の側面は、

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引きシステムにおいて、

前記ユーザデバイスは、クリアリングセンタの発行した発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行する構成を有し、

サービスプロバイダは、前記ユーザデバイスから受信する前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成してクリアリングセンタに送信する処理を実行する構成を有し、

クリアリングセンタは、前記サービスプロバイダから受信する前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するとともに、利用料振替処理要求を口座管理機関に送信する処理を実行する構成を有し、

口座管理機関は、前記振替処理要求に従った口座間の振替処理を実行する構成を有することを特徴とするコンテンツ取り引きシステムにある。

【００１４】

さらに、本発明のコンテンツ取り引きシステムの一実施態様は、前記ユーザデバイスと前記サービスプロバイダは各々暗号処理部を有し、前記ユーザデバイスから前記サービスプロバイダへの利用ログ送信の際は、前記ユーザデバイスと前記サービスプロバイダ間において相互認証処理を実行し、さらに、前記ユーザデバイスは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログ

を受信した前記サービスプロバイダは該電子署名の検証処理を実行する構成であることを特徴とする。

【００１５】

さらに、本発明のコンテンツ取り引きシステムの一実施態様は、前記サービスプロバイダと前記クリアリングセンタは各々暗号処理部を有し、前記サービスプロバイダから前記クリアリングセンタへの受領ログ送信の際は、前記サービスプロバイダと前記クリアリングセンタ間において相互認証処理を実行し、さらに、前記サービスプロバイダは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記クリアリングセンタは該電子署名の検証処理を実行する構成であることを特徴とする。

【００１６】

さらに、本発明のコンテンツ取り引きシステムの一実施態様は、前記クリアリングセンタは、前記ユーザデバイスの電子マネー残高を管理するユーザ残高データベースを有し、該ユーザ残高データベースに登録された電子マネー残高に応じて前記発行ログを生成して前記ユーザデバイスに送信する構成を有することを特徴とする。

【００１７】

さらに、本発明のコンテンツ取り引きシステムの一実施態様は、前記クリアリングセンタと前記ユーザデバイスとは各々暗号処理部を有し、前記クリアリングセンタから前記ユーザデバイスへの発行ログ送信の際は、前記クリアリングセンタと前記ユーザデバイス間において相互認証処理を実行し、さらに、前記クリアリングセンタは、前記発行ログに対して電子署名の生成処理を実行して、前記発行ログを受信した前記ユーザデバイスは該電子署名の検証処理を実行する構成であることを特徴とする。

【００１８】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記販売条件情報は、前記ユーザデバイスによるコンテンツ利用料の配分情報を含み、前記利用ログおよび前記受領ログは前記配分情報を含んで構成され、前記クリアリングセンタは、前記配分情報に基づいてコンテンツ利用料の電子マネーに関す

る精算処理を実行するとともに、前記振替要求の前記口座管理機関に対する送信処理を実行する構成を有することを特徴とする。

【００１９】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記ユーザデバイスに提供されるコンテンツは、暗号化コンテンツと前記販売条件を含むデータにコンテンツ提供者の電子署名がなされたセキュアコンテナ構成を有し、前記ユーザデバイスは前記セキュアコンテナの電子署名の検証を実行して前記セキコンテナの改竄の有無について判定する構成を有することを特徴とする。

【００２０】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記ユーザデバイス、前記サービスプロバイダ、前記クリアリングセンタいずれか相互間におけるログデータの送受信は、公開鍵証明書発行局の発行したデータ送信側の公開鍵証明書を添付して実行する構成であることを特徴とする。

【００２１】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記発行ログは、ユーザデバイス識別子またはユーザ識別子の少なくともいずれかの識別子、および電子マネーによる支払可能な発行金額データを含む発行情報を有することを特徴とする。

【００２２】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記利用ログは、前記発行ログを含み、さらに、コンテンツの利用金額と、利用金額の受け取り先データとを含む利用情報を有することを特徴とする。

【００２３】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記受領ログは、前記利用ログを含み、さらに、コンテンツの利用金額支払元データを含む受領情報を有することを特徴とする。

【００２４】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの

発行要求に基づいて、前記クリアリングセンタが発行する構成であり、前記クリアリングセンタは、前記口座管理機関にあるクリアリングセンタ管理口座に前記ユーザデバイスのユーザからの振り込み済みの金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信する構成を有することを特徴とする。

【００２５】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行する構成であり、前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合、前記ユーザデバイスに対して該ユーザデバイスの電子マネー残高情報を要求し、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信する構成を有することを特徴とする。

【００２６】

さらに、本発明のコンテンツ取り引きシステムの一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行する構成であり、前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合において、前記ユーザデバイスから受領した該ユーザデバイスの電子マネー残高情報に基づいて、発行済みの発行ログに基づく支払い処理の未回収分の存在が判明した場合、シリアル番号の異なる新たな発行ログを、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定して前記ユーザデバイスに対して送信する構成を有することを特徴とする。

【００２７】

さらに、本発明の第２の側面は、

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き方法において、

前記ユーザデバイスは、クリアリングセンタの発行した発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行し、

サービスプロバイダは、前記ユーザデバイスから受信する前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成してクリアリングセンタに送信する処理を実行し、

クリアリングセンタは、前記サービスプロバイダから受信する前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するとともに、利用料振替処理要求を口座管理機関に送信する処理を実行し、

口座管理機関は、前記振替処理要求に従った口座間の振替処理を実行することを特徴とするコンテンツ取り引き方法にある。

【００２８】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記ユーザデバイスと前記サービスプロバイダは各々暗号処理部を有し、前記ユーザデバイスから前記サービスプロバイダへの利用ログ送信の際は、前記ユーザデバイスと前記サービスプロバイダ間において相互認証処理を実行し、前記ユーザデバイスは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記サービスプロバイダは該電子署名の検証処理を実行することを特徴とする。

【００２９】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記サービスプロバイダと前記クリアリングセンタは各々暗号処理部を有し、前記サービスプロバイダから前記クリアリングセンタへの受領ログ送信の際は、前記サービスプロバイダと前記クリアリングセンタ間において相互認証処理を実行し、前記サービスプロバイダは、前記利用ログに対して電子署名の生成処理を実行して、前記利用ログを受信した前記クリアリングセンタは該電子署名の検証処理を実行す

ることを特徴とする。

【００３０】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記クリアリングセンタは、前記ユーザデバイスの電子マネー残高を管理するユーザ残高データベースを有し、該ユーザ残高データベースに登録された電子マネー残高に応じて前記発行ログを生成して前記ユーザデバイスに送信することを特徴とする。

【００３１】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記クリアリングセンタと前記ユーザデバイスとは各々暗号処理部を有し、前記クリアリングセンタから前記ユーザデバイスへの発行ログ送信の際は、前記クリアリングセンタと前記ユーザデバイス間において相互認証処理を実行し、前記クリアリングセンタは、前記発行ログに対して電子署名の生成処理を実行して、前記発行ログを受信した前記ユーザデバイスは該電子署名の検証処理を実行することを特徴とする。

【００３２】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記販売条件情報は、前記ユーザデバイスによるコンテンツ利用料の配分情報を含み、前記利用ログおよび前記受領ログは前記配分情報を含んで構成され、前記クリアリングセンタは、前記配分情報に基づいてコンテンツ利用料の電子マネーに関する精算処理を実行するとともに、前記振替要求の前記口座管理機関に対する送信処理を実行することを特徴とする。

【００３３】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記ユーザデバイスに提供されるコンテンツは、暗号化コンテンツと前記販売条件を含むデータにコンテンツ提供者の電子署名がなされたセキュアコンテナ構成を有し、前記ユーザデバイスは前記セキュアコンテナの電子署名の検証を実行して前記セキュアコンテナの改竄の有無について判定することを特徴とする。

【００３４】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記ユーザ

デバイス、前記サービスプロバイダ、前記クリアリングセンタいずれか相互間におけるログデータの送受信は、公開鍵証明書発行局の発行したデータ送信側の公開鍵証明書を添付して実行することを特徴とする。

【００３５】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、前記クリアリングセンタは、前記口座管理機関にあるクリアリングセンタ管理口座に前記ユーザデバイスのユーザからの振り込み済みの金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信することを特徴とする。

【００３６】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合、前記ユーザデバイスに対して該ユーザデバイスの電子マネー残高情報を要求し、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユーザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定した発行ログを前記ユーザデバイスに対して送信することを特徴とする。

【００３７】

さらに、本発明のコンテンツ取り引き方法の一実施態様において、前記発行ログは、前記ユーザデバイスから前記クリアリングセンタに対する発行ログの発行要求に基づいて、前記クリアリングセンタが発行し、前記クリアリングセンタは、すでに発行済みの発行ログを有するユーザデバイスからの新たな発行ログの発行要求があった場合において、前記ユーザデバイスから受領した該ユーザデバイスの電子マネー残高情報に基づいて、発行済みの発行ログに基づく支払い処理の未回収分の存在が判明した場合、シリアル番号の異なる新たな発行ログを、前記口座管理機関のクリアリングセンタ管理口座に対する前記ユーザデバイスのユー

ザからの振り込み金額と、前記電子マネー残高との加算金額を限度とした発行金額を設定して前記ユーザデバイスに対して送信することを特徴とする。

【００３８】

さらに、本発明の第３の側面は、

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

発行ログに設定された発行金額を限度として、コンテンツの販売条件情報に基づき、電子マネーの残高データからコンテンツ利用料相当額を減額して、利用した金額データを含むコンテンツ利用ログを生成してサービスプロバイダに送信する処理を実行するステップを有することを特徴とするプログラム提供媒体にある。

【００３９】

さらに、本発明の第４の側面は、

ユーザデバイスにおいて利用可能なコンテンツの取り引き決済処理を実行するコンテンツ取り引き処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

発行ログに設定された発行金額を限度として、コンテンツの利用金額データを含むコンテンツ利用ログを生成するステップ、

前記利用ログに基づいて、コンテンツの利用料情報を含む受領ログを生成するステップと、

前記受領ログに基づいてコンテンツ利用に係る電子マネーに関する精算処理を実行するステップと、

を協動的に実行することを特徴とするプログラム提供媒体にある。

【００４０】

本発明の第３および第４の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピ

ュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯ、ＤＶＤなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００４１】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００４２】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【００４３】

【実施例】

［１．システム概要］

まず、本発明のコンテンツ取り引きシステムの概要について図２を用いて説明する。図２には、情報、すなわち音楽データ、画像データ、ゲーム等の各種プログラム等のコンテンツを利用するユーザデバイス２２０、ユーザデバイス２２０に対してコンテンツを提供するサービスプロバイダ２４０、コンテンツ利用に係る電子マネーの決済処理を実行するクリアリングセンタ２６０と、コンテンツ利用に伴う現実のお金の流れを処理する例えば銀行等の金融機関である口座管理機関２８０が示されている。

【００４４】

なお、図２に示すコンテンツ取り引きシステム構成は一例であり、図２に示す構成以外にも、様々なコンテンツ取り引きシステムが構成され得る。例えばサービスプロバイダ２４０を、実際にコンテンツを作成するコンテンツ提供プロバイ

ダと、コンテンツ提供プロバイダからコンテンツを受領し実際のユーザに配布するコンテンツの流通サービスを提供するサービスプロバイダ等からなる複数構成としてもよい。また、クリアリングセンタ２６０と、口座管理機関２８０とを１つの機関とした構成であってもよい。さらに、図２では、ユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０がそれぞれ１つのみ示されているが、実際にはそれぞれの構成が複数存在することが可能である。また、後段で詳細に説明するが、本発明のコンテンツ取り引きシステムでは、複数の異なるユーザデバイス間でのコンテンツ取り引きを可能とした構成を持つ。

【００４５】

図２において、コンテンツを利用するユーザデバイス２２０は、コンテンツの利用料金を電子マネー２２１を用いて支払う。電子マネー２２１に対する入金処理は、ユーザデバイス２２０を管理する管理ユーザが、必要に応じて銀行等の金融機関である口座管理機関２８０に現金を預けたユーザ口座２８１を開設し、ユーザ口座２８１からクリアリングセンタ管理下のユーザ電子マネー口座２８３へ振り込みを行ない、ユーザの振り込んだ金額を上限として、ユーザの電子マネー２２１に使用可能金額（電子マネー残高）が設定され、振り込みを確認した口座管理機関２８０は電子マネーの決済処理、残高管理等を行なうクリアリングセンタ２６０に、ユーザの振込金額（電子マネーの設定金額）を通知して、電子マネーとして利用可能な金額をクリアリングセンタ２６０が管理する。

【００４６】

クリアリングセンタ２６０は、ユーザデバイス２２０の管理ユーザの使用可能な金額、ユーザの使用するユーザデバイス２２０の識別子等をデータとして持つ電子マネー発行ログをユーザデバイス２２０に送信し、ユーザデバイス２２０は、発行ログ２５１をユーザデバイス２２０内に格納する。発行ログ２５１については、後段で詳細に説明する。

【００４７】

ユーザデバイス２２０は、音楽データ、画像データ、ゲーム等の各種プログラム等のコンテンツをサービスプロバイダ２４０から提供を受ける際、電子マネー

２２１を用いてサービスプロバイダ２４０にコンテンツの利用料金の支払いを行なう。この際、電子マネー２２１の残高から利用料金を減額する。また、ユーザデバイス２２０は、発行ログ情報と、コンテンツの利用金額、コンテンツの利用料金の受け取り先情報等を記録したデータからなる利用情報をデータとして持つ利用ログ２５２をサービスプロバイダ２４０に送信する。

【００４８】

サービスプロバイダ２４０は、ユーザデバイス２２０から受領した利用ログ２５２の検証処理を実行して、利用ログ２５２に基づいて、コンテンツ利用料金の支払元、受領日時等からなる受領情報を持つ受領ログ２５３を生成してクリアリングセンタ２６０に送信する。この際、クリアリングセンタ２６０は、決済処理に関する実際の現金の受け渡し情報（配分情報）を口座管理機関２８０に振替要求として送信し、口座管理機関２８０は、クリアリングセンタ２６０からの振替要求に基づいて、サービスプロバイダ口座２８２、クリアリングセンタ２８３相互間において、金額振替を実行する。

【００４９】

なお、図２では、説明の複雑化をさけるためにユーザデバイス２２０の管理ユーザのユーザ口座２８１、サービスプロバイダ口座２８２、クリアリングセンタ２８３のみが示されているが、口座管理機関２８０は、コンテンツ作成者の口座、あるいは、コンテンツの販売店舗等の口座等を持ち、それぞれに予め定められた設定に従って振替を行なう構成としてもよい。これらの料金振替設定情報をコンテンツと共に流通させる形態については、後段で説明する。

【００５０】

［２．ユーザデバイス］

図３に本発明のコンテンツ取り引きシステムに使用されるユーザデバイスの一実施例に係る構成ブロック図を示す。ユーザデバイス３００は、コンテンツを格納する記録デバイス３５０を持つ。

【００５１】

ユーザデバイス３００は、例えばパーソナル・コンピュータ（ＰＣ：Personal Computer）、あるいはゲーム機器等によって構成される。ユーザデバイス３０

０は、ユーザデバイス３００における暗号処理時の記録デバイス３５０との通信制御を含む統括的制御を実行する制御部３０１、暗号処理全般を司る記録再生器暗号処理部３０２、記録再生器に接続される記録デバイス３５０と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ３０３、ＤＶＤなどのメディア３６０から少なくともデータの読み出しを行う読み取り部３０４、外部とデータの送受信を行う通信部３０５を有する。

【００５２】

ユーザデバイス３００は、制御部３０１の制御により記録デバイス３５０に対するコンテンツデータのダウンロード、記録デバイス３５０からのコンテンツデータ再生を実行する。記録デバイス３５０は、ユーザデバイス３００に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、ＥＥＰＲＯＭ、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成される外部メモリ３５２を有する。

【００５３】

ユーザデバイス３００は、図３の左端に示す記憶媒体、ＤＶＤ、ＣＤ、ＦＤ、ＨＤＤに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部３０４、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部３０５を有し、外部からコンテンツを入力する。

【００５４】

ユーザデバイス３００は、電子マネー３１０をデバイスに固定、あるいは着脱可能に有しており、利用情報、残高金額等をフラッシュメモリ、ＥＥＰＲＯＭ等で構成されるメモリ３１３に記憶する。電子マネー３１０が外部と通信するデータは、電子マネーを所有する個人ＩＤ、利用金額等であり、これらが暗号化されて電子マネー３１０に入出力する。これらのデータの暗号処理を実行するのが暗号処理部３１２でありデータ入出力制御、暗号処理部での処理制御を制御部３１１が実行する。電子マネー３１０は、例えばセキュリティ用ＩＣカードのようなＳＡＭ：Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅとして構成される。

【００５５】

さらに、ユーザデバイス３００は、ＳＡＭにより構成された暗号処理部３０２を有する。なお、図３の例では、暗号処理部３０２のＳＡＭと電子マネー３１０のＳＡＭとが別構成として示されているが、これらのＳＡＭは１つのモジュールとして構成してもよい。暗号処理部３０２は、読み取り部３０４または通信部３０５を介して外部から入力されるコンテンツデータを記録デバイス３５０にダウンロード処理する際、あるいはコンテンツデータを記録デバイス３５０から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。さらに、コンテンツの利用料金の支払い情報として発行する発行ログの受領、利用ログの生成処理、送信処理等の際の認証処理、暗号処理、データの検証処理等を実行する。暗号処理部３０２は、暗号処理部３０２全体を制御する制御部３０６、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ３０７、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部３０８から構成されている。

【００５６】

暗号処理部３０２、電子マネー３１０部は、ＳＡＭ：Secure Application Moduleによって構成することで、不正なデータの書き換えを防止することができる。暗号処理部３０２、電子マネー３１０部には、セキュリティの高い情報として、ユーザデバイス３００の識別子（ＩＤ）、電子マネーの残高、後述する電子マネー発行ログ、さらに、認証処理、暗号処理等に用いる各種の鍵情報が格納される。なお、後段で説明するが、電子マネー発行ログには電子マネーによる利用可能な金額に相当する発行金額が記録されユーザデバイスに格納される。

【００５７】

制御部３０１は、例えば、ユーザデバイス３００と通信部３０５を介して通信手段に接続されたサービスプロバイダと暗号処理部３０２との相互認証処理の仲介処理、セッション鍵で暗号化されて送付されるコンテンツ鍵の暗号処理部３０２における復号処理における仲介制御、さらに記録デバイス３５０が装着された際に記録デバイスコントローラ３０３を介して記録デバイス３５０に初期化命令

を送信したり、あるいは、暗号処理部３０２の暗号／復号化部３０８と記録デバイス暗号処理部３５１間で行われる相互認証処理、署名検証処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。

【００５８】

暗号処理制御部３０６は、ユーザデバイス３００において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、サービスプロバイダとの相互認証処理の制御、ユーザデバイス３００と記録デバイス３５０との間で実行される認証処理の制御、暗号処理部３０２の暗号／復号化部３０８において実行される各種処理、例えばコンテンツ鍵（コンテンツ暗号化鍵）の鍵交換処理、ダウンロード、あるいは再生コンテンツデータに関する暗号処理の実行命令等、暗号処理全般に関する制御を行なう。

【００５９】

内部メモリ３０７は、ユーザデバイス３００において実行される相互認証処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは記録再生器の識別データ等を格納する。記録再生器の識別データは、例えばサービスプロバイダとの相互認証処理等において用いられる。

【００６０】

暗号／復号化部３０８は、内部メモリ３０７に格納された鍵データ等を使用して、外部から入力されるコンテンツデータおよび電子マネーを使用した利用金支払い処理に伴うデータ転送時の認証処理、暗号化処理、復号化処理、データの検証、乱数の発生などの処理を実行する。

【００６１】

暗号処理部３０２の内部メモリ３０７は、暗号鍵などの重要な情報を持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部３０２は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【００６２】

ユーザデバイス３００は、これらの暗号処理機能の他に、中央演算処理装置（メインＣＰＵ：Central Processing Unit）３２１、ＲＡＭ（Random Access Memory）３２２、ＲＯＭ(Read Only Memory)３２３、ＡＶ処理部３２５、入力インタフェース３２４、ＰＩＯ（パラレルＩ／Ｏインタフェース）３２６、ＳＩＯ（シリアルＩ／Ｏインタフェース）３２７を備えている。

【００６３】

中央演算処理装置（メインＣＰＵ：Central Processing Unit）３２１、ＲＡＭ（Random Access Memory）３２２、ＲＯＭ(Read Only Memory)３２３は、ユーザデバイス３００本体の制御系として機能する構成部であり、主として暗号処理部３０２で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインＣＰＵ：Central Processing Unit）３２１は、制御部３０１の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをＡＶ処理部３２５へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【００６４】

ＲＡＭ３２２は、ＣＰＵ３２１における各種処理用の主記憶メモリとして使用され、メインＣＰＵ３２１による処理のための作業領域として使用される。ＲＯＭ３２３は、メインＣＰＵ３２１で起動されるＯＳ等を立ち上げるための基本プログラム等が格納される。

【００６５】

ＡＶ処理部３２５は、具体的には、例えばＭＰＥＧ２デコーダ、ＡＴＲＡＣデコーダ、ＭＰ３デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【００６６】

入力インタフェース３２４は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインＣＰＵ３２１に出力する。メインＣＰＵ３２１は、例えば実行中のゲームプログラム等に基づいて使用者からのコ

ントローラからの指示に従った処理を実行する。

【００６７】

ＰＩＯ（パラレルＩ／Ｏインタフェース）３２６、ＳＩＯ（シリアルＩ／Ｏインタフェース）３２７は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

【００６８】

記録デバイス３５０は、例えばユーザデバイス３００に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス３５０は暗号処理部３５１、外部メモリ３５２を有する。

【００６９】

記録デバイス暗号処理部３５１は、ユーザデバイス３００からのコンテンツデータのダウンロード、または記録デバイス３５０からユーザデバイス３００へのコンテンツデータの再生処理時等におけるユーザデバイス３００と記録デバイス３５０間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、ユーザデバイス３００の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。外部メモリ３５２は、前述したように、例えばＥＥＰＲＯＭ、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきＲＡＭなどによって構成されコンテンツデータの格納、コンテンツ鍵の格納等に使用される。

【００７０】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツを提供するサービスプロバイダは、提供コンテンツを暗号化して、ＣＤ，ＤＶＤ等のメディア、あるいはネットワークを介してユーザに提供する。コンテンツの利用料金は、ネットワーク等の通信手段を介して電子マネーにより支払われる。

【００７１】

［３．コンテンツ取り引きシステムにおける決済処理］

（３－１）概要

図４は、本発明のコンテンツ取り引きシステムにおけるユーザデバイス２２０

、サービスプロバイダ２４０、クリアリングセンタ２６０と、口座管理機関２８０において実行されるコンテンツ利用料金の決済に伴うデータ転送を説明する図である。

【００７２】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０と、口座管理機関２８０相互間で実行されるデータ転送は、基本的に通信内容の漏洩を防止するために通信データの暗号化処理を施して実行する。また、データ送信に先立ち、通信相互間において相互認証処理が実行されて認証が成立した場合にのみ、例えば電子マネーによる支払いデータ等を暗号化データとして送信する。認証処理については後段で説明する。

【００７３】

図４に示す公開鍵証明書発行局（ＩＡ：Ｉｓｓｕｅｒ　Ａｕｔｈｏｒｉｔｙ）４１０は、ユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０と、口座管理機関２８０相互で行われる暗号文書の通信に用いられる各々の公開鍵を証明するための第三者機関であり、各々の公開鍵の証明書を発行する認証局としての役割を有する。

【００７４】

ユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０は、図４に示すように、それぞれ、公開鍵証明書発行局（ＩＡ）４１０の公開鍵を有する。さらに、ユーザデバイス２２０は、ユーザデバイス固有の公開鍵情報を記録したユーザデバイス証明書、さらにユーザデバイス２２０を使用するユーザ固有の公開鍵情報を記録したユーザ証明書を公開鍵証明書発行局４１０から受領し格納している。

【００７５】

公開鍵証明書は、公開鍵暗号方式における暗号処理の信頼性を維持するためのものである。公開鍵証明書は、例えばユーザデバイスであればユーザデバイスＩＤと公開鍵等を公開鍵証明書発行局（ＩＡ）４１０に提出することにより、公開鍵証明書発行局（ＩＡ）４１０が公開鍵証明書発行局（ＩＡ）のＩＤや有効期限

等の情報を付加し、さらに公開鍵証明書発行局（ＩＡ）による署名を付加して作成する証明書である。または、サービスを提供するサービスプロバイダが保持する登録局（（ＲＡ）：Registration Auyhority）にユーザデバイスＩＤと公開鍵を提出し、登録を申請し、登録局（ＲＡ）が公開鍵証明書発行局（ＩＡ）に対して発行依頼を行なってユーザデバイスに公開鍵証明書を送付する構成としてもよい。

【００７６】

図５に公開鍵証明書の例を示す。図５に示すように公開鍵証明書には、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、公開鍵証明書発行局（ＩＡ）の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。

【００７７】

電子署名は、証明書のバージョン番号、公開鍵証明書発行局（ＩＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、公開鍵証明書発行局（ＩＡ）の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して公開鍵証明書発行局（ＩＡ）の秘密鍵を用いて生成したデータである。

【００７８】

公開鍵証明書発行局（ＩＡ）４１０は、図５に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（リボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【００７９】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（ＩＡ）の公開鍵（ＩＡ公開鍵）を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者、すな

わち図４では、ユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０は、共通の公開鍵証明書発行局（ＩＡ）の公開鍵を保持している必要がある。

【００８０】

図４に示すように、ユーザデバイス２２０は、ＩＡ公開鍵と、ユーザデバイス証明書、ユーザ証明書を有し、サービスプロバイダ２４０は、ＩＡ公開鍵と、サービスプロバイダ証明書、クリアリングセンタ２６０は、ＩＡ公開鍵と、クリアリングセンタ証明書、口座管理機関２８０は、ＩＡ公開鍵と、口座管理機関証明書とを有している。これらユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０の相互間においては、各証明書を用いた公開鍵暗号方式、あるいは共通鍵暗号方式を用いた通信を実行して、コンテンツ利用料金の支払い、決済処理用のデータを転送する。なお、口座管理機関２８０への通信は既存のＳＳＬ(Secure Socket Layer)等を用いた通信としてもよい。

【００８１】

（３－２）コンテンツ料金処理において使用される各種ログ

本発明のコンテンツ取り引きシステムにおいては、コンテンツの利用料金の決済処理のための情報、具体的には、コンテンツ利用に関する各種の取り引き情報を記録した各種のログ情報が図２で説明したユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０間で転送される。すなわちユーザデバイス２２０が有する発行ログ２５１、ユーザデバイス２２０がコンテンツ利用料金支払い時に生成してサービスプロバイダ２４０に送信する利用ログ２５２、サービスプロバイダ２４０が利用ログ２５２に基づいて生成してクリアリングセンタ２６０に送信する受領ログ２５３である。ここでは、これらの各ログについて図６を用いて説明する。

【００８２】

ユーザデバイス２２０の有する発行ログは、図２に示すクリアリングセンタ２６０が発行した電子マネー情報であり、発行ログに記録された情報に対して発行ログの発行者（例えばクリアリングセンタ）の署名（電子署名）がなされ、発行

ログの記録データの改竄が防止されている。発行ログには、図６に示すように、電子マネーにおいて利用可能な総金額に相当する発行金額、ユーザデバイスまたは利用者の識別子であるユーザデバイスＩＤまたはユーザＩＤ、有効期限、発行ログの発行者(例えばクリアリングセンタ)が管理するシリアル番号が記録されている。

【００８３】

発行ログは、利用者の要求に基づいて発行者（クリアリングセンタ）が発行する。例えばユーザがクリアリングセンタ２６０の管理口座のある銀行に出向き、クリアリングセンタの管理口座に利用希望額を振り込んだり、あるいはクレジットカードを使用して振り込みを行なうことで実際の金額移動を行なう。クリアリングセンタ２６０は、銀行から振り込み情報を受け取って振り込みの確認を行ない、振り込み金額に対応する金額を発行ログの発行金額として設定する。あるいは、ユーザから直接クリアリングセンタ２６０に発行ログの発行要求と、ユーザの銀行口座からクリアリングセンタ２６０の管理口座への振替依頼を行なって、クリアリングセンタ２６０が銀行に対して振り替え要求を行なって、振替金額に応じた発行金額を設定した発行ログを発行する構成としてもよい。

【００８４】

ユーザデバイス２２０は、クリアリングセンタ２６０の発行した発行ログに設定された発行金額を限度として、コンテンツの利用料金を電子マネー２２１を用いて支払う。電子マネー２２１によるの支払い処理の際には、ＳＡＭによって構成される電子マネー２２１に記録されている電子マネー残高がチェックされ、残高が支払い金額より少ない場合は、電子マネー２２１による支払いは実行できない。残高が支払い金額以上である場合にのみ電子マネーによる支払いが実行される。電子マネー２２１に記録されている発行ログに基づく電子マネー使用可能残高は、支払処理により更新される。

【００８５】

発行ログに設定された発行金額に相当する金額を使いきった場合、すなわち発行ログに基づく電子マネー使用可能残高が０になったユーザは、所定の金額をクリアリングセンタ管理口座に振り込んで新たな発行ログの発行をクリアリングセ

ンタに要求することができる。また、残高が０にならない場合であっても、ユーザは新たな発行ログの追加発行をクリアリングセンタ２６０に要求することができる。

【００８６】

クリアリングセンタ２６０による発行ログの追加発行処理について説明する。まず、ユーザは追加利用する金額をクリアリングセンタ管理口座に振り込みクリアリングセンタ２６０に、発行ログの追加発行を要求する。クリアリングセンタ２６０は、発行ログの追加発行を要求してきたユーザデバイスから、すでに発行済みの「発行ログ－ｏｌｄ」と、電子マネー２２１に記録されている「発行ログ－ｏｌｄ」に基づく電子マネー使用可能残高データの送信を要求し、これらのデータを受領する。クリアリングセンタ２６０は、ユーザの振り込み金額と、ユーザから受信した「発行ログ－ｏｌｄ」に基づく電子マネー使用可能残高との合計を新たな発行ログである「発行ログ－ｎｅｗ」の発行金額として設定して新たな発行ログ「発行ログ－ｎｅｗ」をユーザデバイスに送信する。

【００８７】

上述の処理において、クリアリングセンタ２６０は、ユーザから受信する「発行ログ－ｏｌｄ」に基づく電子マネー使用可能残高が、クリアリングセンタ２６０内のユーザ残高管理サーバの残高データと一致しない場合がある。これは、受領ログの精算処理が遅れて行われる場合があるからである。この場合、クリアリングセンタ２６０は、ユーザＩＤと発行ログシリアル番号と、各発行ログに対する残高をユーザ残高管理サーバ２６３において管理し、第2の発行ログの追加発行をする。例えば「発行ログ－ｏｌｄ」の発行金額が￥１０，０００で、￥８，０００が利用済みで、ユーザデバイス２２０の電子マネーの残高データが￥２，０００であるとき、クリアリングセンタ２６０において、￥５，０００の受領ログ精算のみが処理済であるとすると、￥３，０００の未処理金額があることになる。ここで、ユーザデバイス２２０が新たに￥２０，０００の発行ログの追加発行要求を行なったとする。

【００８８】

この時点において、クリアリングセンタ２６０が発行金額の￥２０，０００の

「発行ログ－ｎｅｗ」を発行すると、クリアリングセンタ２６０のユーザ残高管理サーバ２６３の当該ユーザの発行ログ関連データは、［発行ログ－ｏｌｄ：ユーザＩＤ：残高￥５，０００］と、［発行ログ－ｎｅｗ：ユーザＩＤ：残高￥２０，０００］となる。その後、クリアリングセンタ２６０が、未回収分の￥３，０００の受領ログの精算を行なった場合は、［発行ログ－ｏｌｄ：ユーザＩＤ：残高￥２，０００］と、［発行ログ－ｎｅｗ：ユーザＩＤ：残高￥２０，０００］となる。なお、いずれの発行ログに基づく受領ログであるかは、発行ログシリアル番号で区別可能である。また、クリアリングセンタ２６０は、ユーザから受信した「発行ログ－ｏｌｄ」に基づく電子マネー使用可能残高データを受信した際に未回収残高（上記の例では￥３，０００）を未回収残高データとして設定して精算処理を実行するようにしてもよい。

【００８９】

ユーザデバイス２２０は、コンテンツの利用料金を電子マネー２２１を用いて支払う処理を実行すると、利用ログを生成して、これをサービスプロバイダ２４０に送信する。利用ログには、ユーザデバイス２２０の有する発行ログ情報に加えて、利用情報として、コンテンツの対価として支払った金額に対応する利用金額、料金の受け取り先情報、さらに、ユーザデバイス側で管理するシリアル番号が記録されている。なおさらに、ユーザの電子マネーの現在の残高情報と利用サービス情報を付加する構成としてもよい。これらの情報に対してユーザデバイス２２０の署名（電子署名）がなされてユーザデバイス２２０からサービスプロバイダ２４０に送信される。ユーザデバイス２２０は、利用ログをサービスプロバイダ２４０に送信するとともに、利用ログをＳＡＭ外部の記憶手段に格納する。

【００９０】

さらに、サービスプロバイダ２４０は、利用ログに基づいて受領ログを生成して、これを電子マネーの決済処理を行なうクリアリングセンタ２６０に送信する。受領ログは、図６に示すように、利用ログ情報に加えて、受領情報として、料金の支払元情報、受領日時、受領者（本例ではサービスプロバイダ）の管理するシリアル番号が記録されている。これらの情報に対して受領者（サービスプロバイダ２４０）の署名（電子署名）がなされてサービスプロバイダ２４０からクリ

アリングセンタ２６０に送信される。サービスプロバイダ２４０は、受領ログをクリアリングセンタ２６０に送信するとともに、受領ログをＳＡＭ外部の記憶手段に格納する。

【００９１】

なお、コンテンツがユーザ間で取り引きされる場合は、受領ログにはサービスプロバイダの署名ではなく、コンテンツを供給したユーザの署名がなされる。ユーザ間のコンテンツ取り引き（二次配信）については、後段で説明する。

【００９２】

上記の説明および図４で示すように利用ログは、その生成者であるユーザデバイス２２０からサービスプロバイダ２４０に送信されるとともにユーザデバイス２２０内に格納され、受領ログは、その生成者であるサービスプロバイダ２４０からクリアリングセンタ２６０に送信されるとともに、サービスプロバイダ２４０内に格納される。これらのログ保存は、後日振込報告、支払報告等があった場合に、照合処理を実行可能とするためである。各ログをＳＡＭ内に保存しないのは、同一のログがクリアリングセンタ２６０に保管されており、万が一改竄された場合でも正しいログ情報をクリアリングセンタ２６０の保管ログから取り出すことが可能であるからである。

【００９３】

（３－３）電子署名

これら各ログに付加される電子署名について簡単に説明する。まず、電子署名データの生成処理方法の例の１つとして共通鍵暗号方式におけるＤＥＳを用いた例を説明する。なお、本発明においては、ＤＥＳ以外にも、同様の共通鍵暗号方式における処理として例えばＦＥＡＬ（Fast Encipherment ALgorithm：ＮＴＴ）、ＡＥＳ（Advanced Encryption Standard：米国次期標準暗号）等を用いることも可能である。

【００９４】

一般的なＤＥＳを用いた電子署名の生成方法を図７を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを８バイト単位に分割する（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）

。そして、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮが電子署名になる。この値は一般にはメッセージ認証符号（ＭＡＣ（Message Authentication Code））と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをＣＢＣ（Cipher Block Chaining）モードと呼ぶ。このＭＡＣ値の検証時には、検証者が生成時と同様の方法でＭＡＣ値を生成し、同一の値が得られた場合、検証成功とする。

【００９５】

本発明のコンテンツ取り引きシステムにおいて使用される発行ログ２５１、利用ログ２５２、受領ログ２５３には、図６で説明した各種情報が含まれ、これらが検証対象のメッセージに対応する。従って、これらのデータ、あるいはこれらのデータに基づいて生成されるデータを図７に示すＤＥＳ暗号処理部に入力するメッセージとして電子署名を生成する。

【００９６】

次に、公開鍵暗号方式を用いた電子署名の生成方法を図８を用いて説明する。図８に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【００９７】

図８の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2 = x^3 + ax + b$）、Ｇを楕円曲線上のベース

ポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージＭのハッシュ値を計算し、f=Hash(M)とする。

【００９８】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【００９９】

続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【０１００】

【数１】

P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Qとすると、

P≠Qの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Qの時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【０１０１】

これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算

方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する2^{i}×Ｇ（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【０１０２】

ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【０１０３】

ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【０１０４】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図９を用いて説明する。ステップＳ１１で、Ｍをメッセージ、pを標数、a、bを楕円曲線の係数（楕円曲線：$y^{2}=x^{3}+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Gを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージＭのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２=ｃｈ　ｍｏｄ　ｒを計算する。

【０１０５】

ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図８のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判

定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であることが判明している）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【０１０６】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【０１０７】

ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【０１０８】

ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【０１０９】

本発明のコンテンツ取り引きシステムにおいては、例えばユーザデバイス２２０がコンテンツの利用料金を電子マネー２２１を用いて支払う際に、利用ログ２５１を生成サービスプロバイダ２４０に送付する。この利用ログにはユーザデバイスの署名が付加されて、サービスプロバイダ２４０によって検証処理がなされる。またサービスプロバイダ２４０が生成してクリアリングセンタ２６０に送付する受領ログにはービスプロバイダの署名が付加されて、クリアリングセンタ２６０によって検証処理がなされる。またクリアリングセンタ２６０が発行して、ユーザデバイス２２０に送信する発行ログにはクリアリングセンタの署名が付加されてユーザデバイス２２０において検証処理が実行される。

【０１１０】

（３－４）シリアル番号の付与方法

前述の図６の説明において、発行ログ、利用ログ、受領ログのそれぞれにはそれぞれのログ生成者、すなわち、発行ログであればクリアリングセンタ、利用ログであればユーザデバイス、受領ログであればサービスプロバイダ固有のシリアル番号が付与される。このシリアル番号の付与方法の一例を説明する。各ログ生成者は固有の秘密鍵Ｋ（例えばＳＡＭ内に保管）と、付与済みのシリアル番号Ｎ１を用いて次のシリアル番号Ｎ２を生成する。例えばＮ２＝ＤＥＳ（Ｋ，Ｎ１）とする。最終的に各ログ情報を含む受領ログを受領するクリアリングセンタ２６０は、シリアル番号を付与するユーザデバイス、サービスプロバイダの秘密鍵Ｋをすべて管理しており、受領ログを受信した際、各ログのシリアル番号をチェックして、不正なシリアル番号の有無を検証する。不正が見つかった場合は、その受領ログに基づく精算処理を中止する。このようにシリアル番号を管理することにより、不正な金額移動を防止することが可能

【０１１１】

（３－５）相互認証処理およびデータ通信

図４に示すユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０の相互間におけるコンテンツ料金の支払いに関するデータ通信は、暗号化データとして送信する。例えば、図６で説明した各種ログの情報を暗号化して転送する。暗号化処理方式としては様々な態様が可能であるが、図５で説明した公開鍵証明書発行局（ＩＡ）４１０の発行した公開鍵証明書を用いた相互認証処理を実行して、相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましい方式である。

【０１１２】

共通鍵暗号方式を用いた相互認証方法を、図１０を用いて説明する。図１０において、共通鍵暗号方式としてＤＥＳを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図１０において、Ａ，Ｂは図４におけるユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０、口座管理機関２８０の通信を実行する２つの構成要素に対応する。

【０１１３】

まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。図７に示すＤＥＳのＣＢＣモード処理構成によれば、ＲａがＭ１、ＲｂがＭ２、ＩＤ（ｂ）がＭ３に相当し、初期値：ＩＶ＝０としたときの出力Ｅ１、Ｅ２、Ｅ３が暗号文となる。

【０１１４】

これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【０１１５】

次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【０１１６】

これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【０１１７】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認

証が失敗したものとして処理を中断する。

【０１１８】

次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１１を用いて説明する。図１１において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１１において、まずＢが、６４ビットの乱数Ｒｂを生成し、Aに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇを生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。電子署名の生成方法は図８で説明したので、その詳細は省略する。

【０１１９】

公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（ＩＡ）４１０の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（ＩＡ）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図９で説明したのでその詳細は省略する。

【０１２０】

図１１に戻って説明を続ける。Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証方法は図９で説明したので、その詳細は省略する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【０１２１】

次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【０１２２】

Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ｂｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【０１２３】

両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【０１２４】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【０１２５】

ユーザデバイス２２０、サービスプロバイダ２４０、クリアリングセンタ２６０と、口座管理機関２８０は、このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【０１２６】

ユーザデバイス２２０がコンテンツをサービスプロバイダ２４０に要求してコンテンツを受領する際のコンテンツ料金の支払処理は、電子マネー２２１の残高

からコンテンツ料金を減額して、さらに、利用ログ情報として必要な情報、すなわち、コンテンツの対価として支払った金額に対応する利用金額、料金の受け取り先情報、利用サービス情報、さらに、ユーザデバイス側で管理するシリアル番号等を記録した利用ログを生成してサービスプロバイダ２４０へ送信する処理となる。

【０１２７】

図４に戻り、本発明のコンテンツ取り引きシステムにおけるコンテンツの取り引き処理について説明を続ける。

【０１２８】

ユーザデバイス２２０は、コンテンツの提供者であるサービスプロバイダ２４０に対してコンテンツを要求（図４に示す（１）の処理）する。

【０１２９】

サービスプロバイダ２４０は、ユーザデバイス２２０から要求のあったコンテンツをユーザデバイスに送信（図４に示す（２）の処理）する。なお、ここで送信するコンテンツは、コンテンツデータをコンテンツ鍵によって暗号化した暗号化コンテンツである。サービスプロバイダ２４０は、暗号化コンテンツに加えて、コンテンツ料金およびコンテンツ料金の支払先情報としてのコンテンツの価格情報、さらに後段で説明するが、コンテンツの利用期限、複製可能回数等を販売条件情報（ＵＣＰ：Usage Control Policy）として設定して、さらに電子署名を付してユーザデバイスに送信する。サービスプロバイダ２４０は、コンテンツの利用条件を各種設定可能である。これらの転送コンテンツ構成（セキュアコンテナ）については後段で説明する。

【０１３０】

次に、ユーザデバイス２２０は、予め定められたコンテンツの使用料金に対応する金額を電子マネー２２１から引出してサービスプロバイダ２４０に支払う。

【０１３１】

これらの料金処理は、具体的には、図４に示すユーザデバイス２２０の有する電子マネー２２１の残高から利用料金を減額し、発行ログ情報と、コンテンツの利用金額、コンテンツの利用料金の受け取り先情報等を記録したデータからなる

利用情報をデータとして持つ利用ログ２５２を生成してサービスプロバイダ２４０に送信（図４に示す（３）の処理）する処理として実行される。この利用ログデータの転送は、上述した通り、ユーザデバイス２２０とサービスプロバイダ２４０間の相互認証処理を実行し、ユーザデバイス２２０による電子署名がなされて転送する。

【０１３２】

サービスプロバイダ２４０は、ユーザデバイス２２０から受領した利用ログ２５２を検証して、データ正当性が確認されると、暗号化コンテンツの復号に用いるコンテンツ鍵を先に説明した認証処理の際に生成したセッション鍵で暗号化してユーザデバイス２２０に送信する。ユーザデバイスは、暗号化コンテンツ鍵をセッション鍵で復号して得たコンテンツ鍵を用いて暗号化コンテンツを復号して利用する。

【０１３３】

サービスプロバイダ２４０は、さらに、ユーザデバイス２２０から受領した利用ログ２５２に基づいて、図６で説明したコンテンツ利用料金の支払元、受領日時等からなる受領情報を持つ受領ログ２５３を生成してクリアリングセンタ２６０に送信（図４に示す（４）の処理）する。このデータ転送についても、サービスプロバイダ２４０とクリアリングセンタ２６０間の相互認証処理を実行し、サービスプロバイダ２４０による電子署名を行なってデータ転送が実行される。

【０１３４】

クリアリングセンタ２６０は、サービスプロバイダ２４０から受信した受領ログ２５３を検証して、データ正当性が確認されると、受領ログ２５３に基づいて電子マネーによる支払い処理、すなわち電子データ上での決済処理を行なうことになる。

【０１３５】

まず、クリアリングセンタ２６０は、受領ログ中のデータに基づいてユーザ管理サーバ中の対応するユーザデータを抽出し、クリアリングセンタ２６０が管理するユーザの電子マネーによる支払処理であることを確認する。さらに、クリアリングセンタ２６０は、決済処理に関する実際の現金の受け渡し情報を口座管理

機関２８０に振替要求として送信（図４に示す（５）の処理）する。

【０１３６】

口座管理機関２８０は、クリアリングセンタ２６０からの振替要求に基づいて、サービスプロバイダ口座２８２、クリアリングセンタ管理下のユーザ電子マネー口座２８３相互間において、金額振替、振込処理を実行（図４に示す（６）の処理）する。なお、先に説明したように振込先は１つのプロバイダとは限らず、複数の関係先、例えばコンテンツ著作者、コンテンツ販売店等である場合にはその他の口座２８５に対する振込処理も実行される。また、これらの処理は複数の受領ログに対して一括して行なう場合もある。なお、図４に示す（６）の処理は、各口座が同一金融機関内にあれば、同一の金融機関（例えば銀行）内で行われるが、異なる金融機関に口座が存在する場合は、異なる金融機関の間での金額振替、振込処理として行われる。これらの金額配分に関しては、受領ログ中に記録されており、クリアリングセンタ２６０は、受領ログに記録された配分情報に従った振替要求を口座管理機関２８０に対して行なう。コンテンツ料金の配分については、後段で説明する。

【０１３７】

このコンテンツ利用料金配分情報は、図６の受領ログに含まれる利用ログ中の利用情報中の「受取先」、受領ログ中の受領情報の「支払元」情報であり、クリアリングセンタ２６０がこの情報に基づいて振替構成を決定して、口座管理機関２８０に対して振替要求を行なうことになる。

【０１３８】

口座管理機関２８０による金額移動としての金額振替、振込処理が実行されると、口座管理機関２８０は、振替処理確認応答をクリアリングセンタ２６０に送信（図４に示す（７）の処理）する。

【０１３９】

振替処理確認応答を受信したクリアリングセンタ２６０は、決済サーバ２６２に格納した決済データを更新して電子マネーの決済処理を実行（図４に示す（８）の処理）するとともに、各ユーザの電子マネー残高を登録しているユーザ残高管理サーバ２６３の残高データの更新処理を実行（図４に示す（９）の処理）す

る。これらの処理が正常に実行されると、クリアリングセンタ２６０のユーザ残高管理サーバ２６３の残高と、口座管理機関２８０のクリアリングセンタ管理下のユーザ電子マネー口座２８３との残高が一致することになる。

【０１４０】

［４．二次配布を可能としたコンテンツ構成］

本発明のコンテンツ取り引きシステムでは配布するコンテンツを以下に説明する構成とすることで、複数の異なるユーザ間においてコンテンツの配信を可能とし、かつユーザ間の配信においてもコンテンツ利用料金を回収することが可能とした構成を持つ。

【０１４１】

以下で説明するユーザ間のコンテンツ配信の形態には２つの形態がある。１つは、ユーザＡからユーザＢ、さらにユーザＢからユーザＣ等、直列的に異なるユーザ間をコンテンツが順次、取り引きされる形態である。この直列的なユーザ間のコンテンツ配信を以下、「世代間配信」と呼ぶ。もう１つの配信形態は、ユーザＡの購入したコンテンツをユーザＡからユーザＢ，Ｃ，Ｄ等、並列的に配信する形態である。すなわち１人のユーザから複数のユーザに並列に同一コンテンツを配信する形態である。この並列的なコンテンツ配信を、以下「二次配信」と呼ぶ。

【０１４２】

図１２に本発明のコンテンツ取り引きシステムにおいて流通するコンテンツを含むセキュア・コンテナ（Ｓｅｃｕｒｅ　Ｃｏｎｔａｉｎｅｒ）の構成を示す。図１２に示すようにセキュアコンテナは、コンテンツ鍵によって暗号化されたコンテンツ１２０１と、コンテンツの料金とコンテンツ料金の受け取り先、配分情報を含む価格情報１２０２と、コンテンツの利用条件、例えば「世代間配信」「二次配信」等の転売が禁止されている１回限りの配信が許容されたコンテンツであるとか、複数回の転売が可能であるとか、複数回の転売が可能である場合の転売条件、例えば２回までの「世代間配信」と、３回までの「二次配信」が許容されているコンテンツであるとか、あるいは利用可能期間等の設定情報としての販売条件（ＵＣＰ）１２０３と、セキュアコンテナの作成者の電子署名１２０４を

含んで構成される。

【０１４３】

価格情報１２０２、販売条件１２０３は、コンテンツ製作者、コンテンツプロバイダ、サービスプロバイダ等のいずれかが設定する、電子署名は、コンテンツの流通を管理する機関による署名である。コンテンツの流通を管理する機関がサービスプロバイダであれば、サービスプロバイダの署名となる。

【０１４４】

図１３に販売条件（ＵＣＰ）１２０３の具体的構成例、図１４に価格情報１２０２の具体的構成例を示す。図１３に示すように販売条件（ＵＣＰ）には、コンテンツ識別子（ＩＤ）、コンテンツの利用可能なユーザデバイスを設定した使用可能機器条件、コンテンツの利用可能な地域を設定した地域コード、どのようにコンテンツを利用してよいかを示す利用権タイプ（例えばコンテンツの再生可能回数、コンテンツの複製（ダウンロード）可能回数）、異なるユーザデバイス間での流通可能回数として、前述した「世代間配信」の可能回数を設定した「ＵＣＰ世代管理情報」１３０１と、前述の「二次配信」の可能回数を設定した「二次配信可能回数」１３０２が含まれる。「ＵＣＰ世代管理情報」に設定されたそれぞれのユーザ間での配信可能回数は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報（ＵＣＳ：Usage Control Status）（図１６参照）中の「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」の元データとなり、「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」に基づいてそれぞれの処理の可否が決定される。「ＵＣＳ世代管理情報」はコンテンツの世代間配信毎に更新され、「ＵＣＳ二次配信可能回数」はコンテンツの二次配信毎に更新される。

【０１４５】

ユーザデバイス内のＵＣＳに記録される「ＵＣＳ世代管理情報」に基づいて世代間配信の可否が決定される。すなわち、セキュアコンテンツ内の販売条件（ＵＣＰ）の「ＵＣＰ世代管理情報」に設定された世代間配信可能回数を制限回数としてコンテンツの世代間配信が可能となる。それ以上のコンテンツの世代間配信はエラーとなり、実行されない。同様に、ユーザデバイス内のＵＣＳに記録され

た「ＵＣＳ二次配信可能回数」に基づいて二次配信の可否が決定される。すなわち、セキュアコンテンツ内の販売条件（ＵＣＰ）の「ＵＣＰ二次配信可能回数」に設定された二次配信可能回数を制限回数としてコンテンツの二次配信が可能となる。それ以上のコンテンツの二次配信はエラーとなり、実行されない。

【０１４６】

さらに後段で説明するが、「ＵＣＳ世代管理情報」は、世代間配信、つまりユーザ間のコンテンツ取り引き（セキュアコンテナの転送）の際にユーザ間において継承されてコンテンツの提供を受けたユーザデバイスＢにおいて、コンテンツ供給元のユーザデバイスＡのＵＣＳ（Ａ）に基づいて、ＵＣＳ（Ａ）の「ＵＣＳ世代管理情報」を引き継いだ新たなＵＣＳ（Ｂ）が生成される。例えばＵＣＳ（Ａ）の「ＵＣＳ世代管理情報」が５であったとき、ユーザデバイスＡからユーザデバイスＢに対する世代間配信により、1回の世代間配信が実行されるので、ユーザデバイスＢに生成されるＵＣＳ（Ｂ）の「ＵＣＳ世代管理情報」は４に設定される。これらの処理については、後段で詳細に説明する。

【０１４７】

また、「ＵＣＳ二次配信可能回数」についても、二次配信を行なったユーザ間で、その情報を引き継いで、二次配信を受けたユーザデバイスにおいて、「ＵＣＳ二次配信可能回数」を１つ減少、すなわちデクリメントして新たなＵＣＳを生成して格納する。

【０１４８】

あるいは、二次配信に関しては、ユーザ間での「ＵＣＳ二次配信可能回数」の情報の継承を行なわず、二次配信を受けたユーザデバイスにおいて、セキュアコンテナの「ＵＣＰ二次配信可能回数」を再度有効にする構成としてもよい。すなわち、「ＵＣＰ二次配信可能回数」が５回として設定されている場合、そのコンテンツを新たに受領したユーザは常に５回のコンテンツの二次配信が可能になるように構成してもよい。

【０１４９】

世代間配信と二次配信の継承の例について説明する。サービスプロバイダから最初にコンテンツを購入したユーザ（Ａ）は、セキュアコンテナ中のＵＣＰにあ

る「ＵＣＰ世代管理情報」と「ＵＣＰ二次配信可能回数」に基づいて「ＵＣＳ世代管理情報」と「ＵＣＳ二次配信可能回数」を有するＵＣＳを生成して格納する。例えば「ＵＣＰ世代管理情報」＝３、「ＵＣＰ二次配信可能回数」＝５であったとすると、ユーザＡのＵＣＳは、「ＵＣＳ世代管理情報」＝３、「ＵＣＳ二次配信可能回数」＝５として生成される。

【０１５０】

ユーザ（Ａ）がユーザ（Ｂ）にコンテンツを配信すると、ユーザＡの「ＵＣＳ世代管理情報」＝３、「ＵＣＳ二次配信可能回数」＝４となり、ユーザＢに生成されるＵＣＳは「ＵＣＳ世代管理情報」＝２、「ＵＣＳ二次配信可能回数」＝５（継承する場合４）となる。

【０１５１】

さらに、ユーザ（Ａ）がユーザ（Ｃ）にコンテンツを配信すると、ユーザＡの「ＵＣＳ世代管理情報」＝３、「ＵＣＳ二次配信可能回数」＝３となり、ユーザＣに生成されるＵＣＳは「ＵＣＳ世代管理情報」＝２、「ＵＣＳ二次配信可能回数」＝５（継承する場合３）となる。

【０１５２】

さらに、ユーザ（Ｂ）がユーザ（Ｄ）にコンテンツを配信すると、ユーザＢの「ＵＣＳ世代管理情報」＝２、「ＵＣＳ二次配信可能回数」＝４（継承している場合３）となり、ユーザＤに生成されるＵＣＳは「ＵＣＳ世代管理情報」＝１、「ＵＣＳ二次配信可能回数」＝５（継承する場合３）となる。

【０１５３】

さらに、ユーザ（Ｄ）がユーザ（Ｅ）にコンテンツを配信すると、ユーザＤの「ＵＣＳ世代管理情報」＝１、「ＵＣＳ二次配信可能回数」＝４（継承している場合２）となり、ユーザＥに生成されるＵＣＳは「ＵＣＳ世代管理情報」＝０、「ＵＣＳ二次配信可能回数」＝５（継承する場合２）となる。

【０１５４】

ここで、ユーザ（Ｅ）は、「ＵＣＳ世代管理情報」＝０であるので、「ＵＣＳ二次配信可能回数」の設定数に無関係に新たな配信はできない。ユーザ（Ａ）は、ユーザ（Ｂ）と（Ｃ）に配信を行なっており、「ＵＣＳ二次配信可能回数」＝

３であり、あと３回の配信が可能である。また、ユーザ（Ｂ）は、ユーザ（Ｄ）に配信を行なっており、「ＵＣＳ二次配信可能回数」＝４（継承している場合３）であり、あと４回（継承している場合３回）の配信が可能である。また、ユーザ（Ｃ）は、配信を行なっておらず、「ＵＣＳ二次配信可能回数」＝５（継承している場合３）であり、あと５回（継承している場合３回）の配信が可能である。ユーザ（Ｄ）は、ユーザ（Ｅ）に配信を行なっており、「ＵＣＳ二次配信可能回数」＝４（継承している場合２）であり、あと４回（継承している場合２回）の配信が可能となる。

【０１５５】

このように、「ＵＣＳ世代管理情報」＝０になったＵＣＳを持つユーザデバイスは、それ以上、他のユーザデバイスに対してコンテンツの配布が実行できなくなるが、「ＵＣＳ世代管理情報」＝１以上であれば、そのユーザは、「ＵＣＳ二次配信可能回数」に設定された回数のコンテンツ配布が可能となる。

【０１５６】

図１３の販売条件（ＵＣＰ）には、さらに、ルール１～Ｎとして、異なるコンテンツ利用条件が設定されている。これらは、ユーザ、ユーザデバイスに応じて、あるいはユーザが選択可能なコンテンツ利用条件を複数設定したものであり、各ルールに従って例えばコンテンツ価格等が異なるように設定されている。

【０１５７】

図１４は、図１２のセキュアコンテナの価格情報のを例を示すものであり、図１３の販売条件（ＵＣＰ）と同様のコンテンツＩＤ等の情報の他に、価格情報ＩＤ、価格情報バージョンが含まれ、さらに、図１３の販売条件（ＵＣＰ）と同様、ルール１～Ｎとして、異なるコンテンツ利用価格が設定されている。各ルールには、それぞれのコンテンツ利用価格、コンテンツ利益配分情報が設定されている。

【０１５８】

先に、図６で説明した利用ログ、および受領ログのコンテンツ利用料金の支払先に関する情報は、上述したセキュアコンテナの販売条件（ＵＣＰ）、価格情報に基づいて生成されるものである。

【０１５９】

図１２に示すセキュアコンテナを流通コンテンツデータとすることにより、複数のユーザ間での二次配信を可能とした決済処理構成を図１５に示す。

【０１６０】

図１５において、ユーザデバイスＡは、サービスプロバイダ２４０に対してコンテンツの要求を行ない、前述したと同様の認証処理、署名検証処理等を実行して、コンテンツ利用料金の支払い処理として発行ログＡ１５３１に基づいて利用ログＡ１５３２を生成してサービスプロバイダ２４０に送信する。

【０１６１】

なお、この転送コンテンツは、図１２で説明したように、コンテンツ鍵で暗号化されたものであり、サービスプロバイダ２４０は、利用ログＡの署名検証を確認した後、ユーザデバイスＡ１５１０に対して、コンテンツ鍵を暗号化して送信する。暗号化処理用の鍵としては、認証処理時に生成するセッション鍵を使用する。具体的な処理の流れを簡単に説明すると、（１）サービスプロバイダ２４０とユーザデバイスＡ１５１０間での相互認証処理、（２）サービスプロバイダ２４０からユーザデバイスＡ１５１０へのセキュアコンテナ送信、（３）ユーザデバイスＡ１５１０におけるセキュアコンテナの署名検証、（４）ユーザデバイスＡ１５１０において、販売条件（ＵＣＰ）、プライスタグ（ＰＴ）から購入判断、（５）ユーザデバイスＡ１５１０の電子マネーで支払処理、（６）サービスプロバイダ２４０からユーザデバイスＡ１５１０へコンテンツ鍵送信、（７）ユーザデバイスＡ１５１０において使用制御情報（ＵＣＳ：Usage Control Status）を生成して保存（コンテンツ鍵保存）の一連の処理となる。なお、サービスプロバイダ２４０とユーザデバイスＡ１５１０間で相互認証処理は、（４）のユーザデバイスＡ１５１０における購入判断処理後、（５）のユーザデバイスＡ１５１０の電子マネーによる支払処理の前に実行するようにしてもよい。

【０１６２】

ユーザデバイスＡ１５１０は、受領したセキュアコンテナの暗号化コンテンツをコンテンツ鍵によって復号して利用することが可能となる。ユーザデバイスＡ１５１０は、コンテンツを利用する際、すなわちコンテンツのコンテンツ鍵を用

いた復号処理の実行に先立ち、ユーザデバイスに格納されたコンテンツ利用の可否の判定に利用されるＵＣＳ（Usage Control Status：使用制御情報）を検査しコンテンツを利用できるか判定する。なお、ＵＣＳは、コンテンツの購入処理、すなわち電子マネーによる支払いをサービスプロバイダ２４０に対して実行する際に、ユーザデバイス内の暗号処理部において、ＵＣＰに基づいて生成され、ユーザデバイス内のメモリに格納される。この処理については、図１６において説明する。ユーザデバイスにおけるセキュアコンテナ格納コンテンツの復号処理は、ＵＣＳを検査した結果、コンテンツを利用できると判定されたときのみ実行可能となる。

【０１６３】

ユーザデバイスの暗号処理部は、ＵＣＳが条件をクリアするものである場合にのみ、コンテンツの復号処理を実行し、ＵＣＳが条件をクリアしない場合には、エラーとして復号処理を実行しない。ユーザデバイスには、このようにユーザデバイスに設定されたＵＣＳが利用条件をクリアした場合にのみ復号処理を実行可能とするコンテンツ利用判定プログラムが格納される。このコンテンツ利用判定プログラムは、例えばセキュアコンテナを提供するサービスプロバイダによって提供され、ユーザデバイスにおいてコンテンツ鍵による復号処理を実行する前ステップで実行するように設定される。

【０１６４】

図１６にコンテンツに応じてユーザデバイスにおいて生成されユーザデバイス内のメモリに格納される使用制御情報（ＵＣＳ：Usage Control Status）の例を示す。図１６に示すように、使用制御情報（ＵＣＳ）には、コンテンツＩＤ、サービスプロバイダＩＤ等の情報の他に、再生残り回数、複製残り回数等のコンテンツ利用の制限情報が含まれる。これら、再生残り回数、複製残り回数は、同一のユーザデバイス内で利用可能な再生残り回数、複製残り回数を示すデータである。さらに使用制御情報（ＵＣＳ）には、「ＵＣＳ世代管理情報」１６０１、および「ＵＣＳ二次配信可能回数」１６０２が含まれる。

【０１６５】

「ＵＣＳ世代管理情報」は前述したように、「世代間配信」の可能回数を設定

したものであり、コンテンツを最初に購入したユーザデバイスは、図１３の「ＵＣＰ世代管理情報」１３０１に一致する回数が設定され、ユーザからの世代間配信によってコンテンツを受領したユーザデバイスは、同一セキュアコンテナについてすでに実行された世代間配信の回数が減じられた回数が設定される。

【０１６６】

「ＵＣＳ二次配信可能回数」１６０２は前述の「二次配信」の可能回数を設定したフィールドであり、コンテンツを最初に購入したユーザデバイスは、図１３の「ＵＣＰ二次配信可能回数」１３０２に一致する回数が設定され、その後の二次配信に応じて更新、すなわち設定回数がデクリメントされる。

【０１６７】

この「ＵＣＳ二次配信可能回数」１６０２は、前述したようにユーザ間のコンテンツ取り引きにおいて、そのデータを継承する構成と、継承しない構成とがある。

【０１６８】

このように、コンテンツのユーザ間での配信は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報（ＵＣＳ：Usage Control Status）中の「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」に基づいて、それぞれの処理の可否が決定される。「ＵＣＳ世代管理情報」はコンテンツの世代間配信毎に更新され、「ＵＣＳ二次配信可能回数」はコンテンツの二次配信毎に更新される。

【０１６９】

同一のセキュアコンテナを異なるユーザ間で転送して取り引きを行なう際、ＵＣＳの「ＵＣＳ世代管理情報」は、コンテンツ提供元からコンテンツ提供先に継承され、コンテンツ提供先において生成されるＵＣＳ内に格納される。「ＵＣＳ二次配信可能回数」は継承する構成と継承しない構成とがある。

【０１７０】

「ＵＣＳ世代管理情報」に記録された利用制限情報は、同一のセキュアコンテナ内のコンテンツについての利用を異なるユーザデバイスで行なった場合も、逐次更新されるデータとなる。例えば、３回の世代間配信制限がセキュアコンテナ

の販売条件（ＵＣＰ）に設定されている場合、最初のセキュアコンテナ購入者（ユーザデバイスＡ）の「ＵＣＳ世代管理情報」には、まず３回の世代間配信が可能として設定されるが、ユーザＡがユーザＢにコンテンツ配信を実行すると、ユーザＢの「ＵＣＳ世代管理情報」は２として設定される。

【０１７１】

このように、セキュアコンテナの販売条件（ＵＣＰ）の「ＵＣＰ世代管理情報」、「ＵＣＰ二次配信可能回数」には、流通回数上限が設定されている。ユーザデバイスに生成されるＵＣＳにも「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」が格納され、前述のコンテンツ利用判定プログラムは、「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」を参照して、設定された流通回数の上限値を超えて、異なるユーザデバイスにセキュアコンテナを送信する場合に、その送信処理の前ステップとして実行されるコンテンツ利用判定プログラムにより、設定回数以上の流通であると判定されると、処理エラーとなりコンテンツの送信処理が実行されない。「ＵＣＰ世代管理情報」、「ＵＣＳ二次配信可能回数」に設定された流通回数の上限値を超えない場合にのみ、コンテンツのユーザデバイス間での送信処理に移行し、コンテンツの世代間配信または二次配信が可能となる。すなわち、ユーザデバイス間での転送（世代間配信または二次配信）は、セキュアコンテナの生成時に販売条件（ＵＣＰ）として設定された「ＵＣＰ世代管理情報」、および「ＵＣＰ二次配信可能回数」での条件の範囲内でのみ可能となる。

【０１７２】

図１５に戻って、ユーザ間でのコンテンツ配信におけるコンテンツ提供ユーザデバイスからの受領ログの発行によるコンテンツ利用料金回収構成について説明する。

【０１７３】

図１５では、まず、サービスプロバイダ２４０から、ユーザデバイスＡに対してセキュアコンテナとしてのコンテンツが提供され、ユーザデバイスＡは、電子マネー１５１１によりコンテンツ利用料金を支払う。具体的には、ユーザデバイスＡは、セキュアコンテナ中の価格情報、販売条件、発行ログＡ１５３１に基づ

いて、利用ログＡ１５３２を生成して、これをサービスプロバイダに転送し、サービスプロバイダ２４０は、利用ログＡ１５３２に基づいて受領ログＡ１５３３を生成してクリアリングセンタ２６０に受領ログＡ１５３３を転送して、クリアリングセンタ２６０が受領ログに基づいて決済処理を行なう。実際の利用料金の振替はクリアリングセンタ２６０の振替要求に基づいて口座管理機関２８０が実行する。

【０１７４】

先に図６を用いて簡単に受領ログの構成について説明したが、受領ログを構成する受領情報の他の具体例を図１７に示す。受領情報には、コンテンツ利用料金の配分情報が含まれる。図１７の受領情報のデータ部１７０１には、コンテンツプロバイダの利益額／利益率、サービスプロバイダの利益額／利益率、その他の関係者の利益額／利益率が記録されている。ここで示す受領情報は一例であり、例えば二次配信を実行したユーザデバイス、あるいはユーザデバイスを管理する管理ユーザに対して利益配分を設定してもよく、あるいはコンテンツの販売がＣＤ、ＤＶＤ等のメディアを介して行われる場合には、その販売店に対する利益配分を設定したり、クリアリングセンタに利益配分を設定したり、あるいはコンテンツ著作者に対する利益配分を設定する構成が可能である。

【０１７５】

これらの受領情報に設定される利益配分情報は、セキュアコンテナの価格情報（図１４参照）、販売条件（図１３参照）に基づいて設定される情報であり、セキュアコンテナの生成時に配分情報を設定してコンテンツを流通させる。クリアリングセンタは、受領情報に記録された配分情報に従って、決済処理構成を構築して、これに基づいて振替要求を口座管理機関２８０に出力し、口座管理機関２８０は要求に従った振替処理を実行する。一方、受領情報としては図６に示すようなものとし、クリアリングセンタ２６０は、売上げのすべてをサービスプロバイダに支払い、サービスプロバイダ２４０がコンテンツプロバイダ、他に利益分配を行なうように構成してもよい。

【０１７６】

また、図１７に示すように受領情報には、セキュアコンテナの販売条件に含ま

れる「ＵＣＰ世代管理情報」１７０２が格納され、クリアリングセンタは、受領情報に記録された「ＵＣＰ世代管理情報」と同一コンテナに基づく受領ログの発行数を比較し、「ＵＣＰ世代管理情報」の設定を超える受領ログについては、その受領ログを無効として処理を行なわない。

【０１７７】

このように、サービスプロバイダ２４０がセキュアコンテナを流通させることにより、セキュアコンテナに記録されたデータに従って、コンテンツの利用がなされ、かつその利用にともなって受領ログが発行されて、発行された受領ログに基づいて正確なコンテンツ利用料金の回収が自動的に行われる。

【０１７８】

さらに、図１５を用いて異なるユーザデバイス間でのコンテンツ流通について説明する。ユーザデバイスＡ１５１０が取得し、例えば所定回数の再生、あるいはダウンロード処理を行なったセキュアコンテナは、異なるユーザデバイスＢ１５２０に転送することが可能である。ただし、世代間配信または二次配信が可能なコンテンツは、前述のようにセキュアコンテナの販売条件の「ＵＣＰ世代管理情報」、「ＵＣＰ二次配信可能回数」が二次配信を可能として設定している場合のみである。この場合、セキュアコンテナは、ユーザデバイスＢ１５２０に転送することが可能である。ただし、転送は前述のように「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」の設定回数の制限範囲内に場合にのみ可能であり、これはコンテンツ利用判定プログラムによって制御されることになる。なお、ユーザデバイス間でのデータ転送においても、前述の認証処理、セッション鍵生成、さらに、転送データの署名検証処理が実行される。

【０１７９】

ユーザデバイスＢ１５２０は、セキュアコンテナを受信し、購入処理を実行すると発行ログＢ１５５１に基づいて、利用ログＢ１５５２を生成して、これをユーザデバイスＡ１５１０に転送し電子マネー１５２１による支払処理を行なう。ユーザデバイスＡ１５１０は、利用ログＢ１５５２に基づいて受領ログＢ１５５３を生成してクリアリングセンタ２６０に受領ログＢを転送して、クリアリングセンタ２６０が受領ログＢに基づいて決済処理を行なう。実際の利用料金の振替

はクリアリングセンタ２６０の振替要求に基づいて口座管理機関２８０が行なう。この場合の受領ログＢにも、前述の図１７で説明したと同様のコンテンツ利用料金配分情報が含まれており、クリアリングセンタ２６０は、受領ログ中のコンテンツ利用料金配分情報に基づいてユーザデバイスＢ１５２０のコンテンツ利用に基づく利用料金配分を実行する。

【０１８０】

セキュアコンテナは、先にも説明したようにコンテナの販売条件（ＵＣＰ）に設定された制限に至るまでユーザ間での流通が可能であり、その範囲内であれば、図１５に示すようにユーザデバイスＢ１５２０から、さらに他のユーザデバイスＣ１５７０にコンテンツを有するセキュアコンテナを流通させることが可能となる。この場合は、ユーザデバイスＢ１５２０が、ユーザデバイスＣ１５７０からの利用ログに基づいて受領ログを生成してクリアリングセンタ２６０に受領ログを送信し、決済を行なう。

【０１８１】

なお、図１５に示すように受領ログは、サービスプロバイダ２４０に送信し、二次配信においては、コンテンツの利用料金の決済処理を行なうのではなく、サービスプロバイダ２４０がコンテンツの提供ユーザに何らかの特典を付与するためのポイントを与えるように構成してもよい。このポイント付与構成については、後段で説明する。

【０１８２】

図１８にユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図を示す。図１８を用いてセキュアコンテナの転送、コンテンツ使用制御情報（ＵＣＳ）生成、格納処理について説明する。

【０１８３】

図１８のサービスプロバイダ１８１０が、セキュアコンテナの最初の流通（一次配布）を行なう。サービスプロバイダ１８１０は、コンテンツデータベース１８１２にコンテンツを格納し、さらに、ユーザ情報データベース１８１３にユーザ情報を格納している。サービスプロバイダ１８１０は、制御部１８１１の制御のもとに暗号処理部１８１４において、セキュアコンテナの転送処理に必要な転

送先との相互認証処理、転送データに対する署名処理等を実行する。暗号処理部１８１４は、これら各暗号処理に必要となる鍵情報、さらに、先に説明した公開鍵証明書発行局（ＩＡ）の公開鍵、公開鍵証明書発行局（ＩＡ）の発行した公開鍵証明書等を保持したメモリを有している。

【０１８４】

また、図１８に示すクリアリングセンタ１８４０がコンテンツ流通に伴うコンテン利用料の決済（電子マネー上のデータ）処理を行なう。クリアリングセンタ１８４０は、通信部１８４５を介して行われる決済用の受領ログ受信または発行ログ送信において各デバイスと認証処理を実行し、また送受信データに対する署名処理、署名検証処理を実行するための暗号処理部１８４４を有し、また、前述の図２、図４等を用いて説明したユーザ管理、ユーザ残高管理用の各種のデータを格納したデータベース１８４２を有する。暗号処理部１８４４には、各暗号処理に必要となる鍵情報、公開鍵証明書発行局（ＩＡ）の公開鍵、公開鍵証明書発行局（ＩＡ）の発行した公開鍵証明書等を保持したメモリを有している。制御部１８４１は、データ送受信、暗号処理部における暗号処理時のデータ転送等の制御を行なう。

【０１８５】

サービスプロバイダ１８１０は、ユーザデバイスＡ１８２０に対してセキュアコンテナを通信部１８１５を介して転送して、ユーザデバイスＡ１８２０が通信部１８２７を介してこれを受信し、購入処理を実行すると、ユーザデバイスＡ１８２０は、制御部１８２１の制御のもとに暗号処理部１８２２においてセキュアコンテナの販売条件（ＵＣＰ）等に基づいてコンテンツ使用制限情報（ＵＣＳ）を生成して、これをフラッシュメモリ等のメモリ１８２４に格納する。

【０１８６】

ユーザデバイスＡ１８２０は、電子マネー１８２８によるコンテンツ利用料金支払処理、すなわち前述した利用ログを暗号処理部１８２２において生成して、通信部１８２７を介してサービスプロバイダ１８１０に送信する。ユーザデバイスＡ１８２０が受信したセキュアコンテナは、ハードディスク等の記憶部１８２５に格納される。サービスプロバイダ１８１０は、ユーザデバイスＡ１８２０か

ら送信された利用ログの検証をして、検証が済むと、コンテンツ鍵をセッション鍵で暗号化してユーザデバイスＡ１８２０に送信する。ユーザデバイスＡ１８２０は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスＡ１８２０固有の保存鍵で暗号化してメモリ１８２４に格納する。

【０１８７】

ユーザデバイスＡ１８２０は、データ再生部１８２６でのコンテンツ再生等、コンテンツ利用に際しては、メモリ１８２４に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部１８２５に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部１８２６において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、その前ステップとして、メモリ１８２４に格納されたコンテンツ使用制限情報（ＵＣＳ）の再生残り回数等の設定条件を判定し、条件がクリアされた場合には復号が可能となる。

【０１８８】

さらに、セキュアコンテナをユーザデバイスＡ１８２０からユーザデバイスＢ１８３０に配信する場合は、ユーザデバイスＡ１８２０は、メモリ１８２４からコンテンツ使用制限情報（ＵＣＳ）を読み出し、暗号処理部１８２２内で保存鍵で復号化（暗号化されていない場合は復号処理は不要）し、ＵＣＳの「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」を判定し、新たな配信が可能と判定された場合には、ユーザデバイスＢ１８３０に対してセキュアコンテナを通信部１８２７を介して転送して、ユーザデバイスＢ１８３０が通信部１８３７を介してこれを受信し、購入処理を実行する。ユーザデバイスＢ１８３０は、制御部１８３１の制御のもとに暗号処理部１８３２においてセキュアコンテナの販売条件（ＵＣＰ）とユーザデバイスＡ１８２０のＵＣＳ情報等に基づいて、新たな「ＵＣＳ世代管理情報」、「ＵＣＳ二次配信可能回数」を設定したコンテンツ使用制限情報（ＵＣＳ－Ｂ）を生成して、これをフラッシュメモリ等のメモリ１８３４に格納する。

【０１８９】

この際に生成するＵＣＳ－Ｂは、前述した通り、ユーザデバイスＡ１８２０の

コンテンツ利用履歴を継承したものとなる。前述の通り、ＵＣＳ－Ｂの「ＵＣＳ世代管理情報」はＵＣＳ－Ａの「ＵＣＳ世代管理情報」より１つ減じた回数として設定される。ＵＣＳ－Ｂの「ＵＣＳ二次配信可能回数」はＵＣＳ－Ａの「ＵＣＳ二次配信可能回数」より１つ減じた回数として設定する構成と、セキュアコンテナ内の「ＵＣＰ二次配信可能回数」と同一回数を新たに設定する構成とがある。

【０１９０】

ユーザデバイスＢ１８３０は、電子マネー１８３８によるコンテンツ利用料金支払処理、すなわち前述した利用ログを暗号処理部１８３２において生成して、通信部１８３７を介してユーザデバイスＡ１８２０に送信する。ユーザデバイスＢ１８３０が受信したセキュアコンテナは、ハードディスク等の記憶部１８３５に格納される。ユーザデバイスＡ１８２０は、ユーザデバイスＢ１８３０から送信された利用ログの検証をして、検証が済むと、メモリ１８２４からコンテンツ鍵を読み出し、これを保存鍵で復号した後、コンテンツ鍵をセッション鍵で暗号化してユーザデバイスＢ１８３０に送信する。ユーザデバイスＢ１８３０は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスＢ１８３０固有の保存鍵で暗号化してメモリ１８３４に格納する。

【０１９１】

また、不正な改竄により設定を超えた使用を行なうと、同一セキュアコンテナに基づいて生成された受領ログ数が、セキュアコンテナ中の販売条件（ＵＣＰ）に含まれる「ＵＣＰ世代管理情報」の設定を超えることとなるため、クリアリングセンタ１８４０に送付された場合に無効と判定される。図１７に示すように受領ログには、コンテンツＩＤ等の情報とともに、セキュアコンテナに記録された「ＵＣＰ世代管理情報」が記録されており、クリアリングセンタ１８４０における決済処理においては、「ＵＣＰ世代管理情報」の設定を超える受領ログを受信した場合はこれを無効とする。なお、ユーザ間配信の認められない設定のなされたコンテンツに基づいて生成された受領ログについても、その受領ログを無効とする処理を実行する。

【０１９２】

ユーザデバイスＢ１８３０は、データ再生部１８３６でのコンテンツ再生等、コンテンツ利用に際しては、メモリ１８３４に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部１８３５に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部１８３６において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、先に説明したように、その前ステップとして、メモリ１８３４に格納されたコンテンツ使用制限情報（ＵＣＳ）に設定された再生残り回数等の利用可能状況が判定され、設定条件範囲内でコンテンツの利用、すなわち復号が可能となる。

【０１９３】

これらの処理により、セキュアコンテナは、サービスプロバイダとユーザデバイス間の一次配布、さらに複数のユーザデバイス間での二次配布（世代間配信または二次配信）が可能となり、そのコンテンツ利用は、セキュアコンテナ中の販売条件（ＵＣＰ）に含まれる「ＵＣＰ世代管理情報」、「ＵＣＰ二次配信可能回数」によって制限された範囲で可能となる。また一次配布、二次配布（世代間配信または二次配信）に伴うコンテンツ利用料金回収もセキュアコンテナ中の価格情報、販売条件等に基づいて生成される受領ログに従って自動的に処理可能となるため、決済処理のための新たな処理が不要となる。

【０１９４】

次に、図１９を用いてコンテンツの世代間配信、二次配信を行なう場合のコンテンツ供給側であるユーザデバイスＡと、コンテンツ受領側であるユーザデバイスＢの主要な処理フローについて説明する。

【０１９５】

まず、ステップＳ１９０１においてユーザデバイスＡとユーザデバイスＢとの間の相互認証処理（図１０、図１１参照）が実行される。この相互認証処理においてセッション鍵が生成される。ステップＳ１９０２において相互認証が成立しなかったと判定された場合は、エラーとなり、その後の処理は継続されない。必要であれば、相互認証処理のリトライを実行する。

【０１９６】

相互認証が成立すると、ステップＳ１９０３においてユーザデバイスＡがハー

ドディスク等の記憶媒体からセキュアコンテナを読み出し、さらにステップＳ１９０４でフラッシュメモリ等のメモリに格納されたコンテンツ使用制限情報（ＵＣＳ（Ａ））を読み出す。

【０１９７】

ステップＳ１９０５において、ユーザデバイスＡは、セキュアコンテナとコンテンツ使用制限情報（ＵＣＳ）とをユーザデバイスＢに送信する。この送信において、ユーザデバイスＡは、送信データに対する署名処理を行なう。なお、コンテンツ使用制限情報（ＵＣＳ（Ａ））全体を送付することは必須ではなく、前述した「ＵＣＳ世代管理情報」等、更新データとして引き継ぐ必要のあるデータのみをコンテンツ使用制限情報（ＵＣＳ（Ａ））から選択してユーザデバイスＢに送付する構成としてもよい。

【０１９８】

ステップＳ１９０６において、ユーザデバイスＢは、ユーザデバイスＡから送付されたセキュアコンテナ、コンテンツ使用制限情報（ＵＣＳ（Ａ））の署名検証を実行する。検証が成立しなかった場合は、エラーとなり、処理は継続せず終了する。

【０１９９】

ステップＳ１９０７において、ユーザデバイスＢは、電子マネーによるコンテンツ利用料金を支払う。この際の支払料金は、セキュアコンテナの価格情報、販売条件に規定されたものとなる。ユーザデバイスＢの具体的な処理は、利用ログを生成してデバイスＡに送付する処理となる。この際、利用ログにはユーザデバイスＢの署名が付加される。

【０２００】

次にステップＳ１９０８において、ユーザデバイスＡがユーザデバイスＢから送付された利用ログの署名検証を実行する。検証が成立しなかった場合は、エラーとなり、処理は継続せず終了する。

【０２０１】

ステップＳ１９０９では、ユーザデバイスＡがメモリから保存鍵（ユーザデバイスＡの暗号処理部のメモリに格納されている）で暗号化されたコンテンツ鍵を

取り出して、保存鍵を用いた復号処理を実行し、さらにセッション鍵（ステップＳ１９０１の認証処理の際に生成）で再暗号化し、ステップＳ１９１０において、セッション鍵で暗号化したコンテンツ鍵をユーザデバイスＢに送信する。

【０２０２】

ステップＳ１９１１において、ユーザデバイスＢは、ユーザデバイスＡから受信したコンテンツ使用制限情報（ＵＣＳ（Ａ））に基づいて、世代管理情報（または世代管理情報＋二次配信可能回数）を引き継いだ新たなコンテンツ使用制限情報（ＵＣＳ（Ｂ））を生成し、さらに、ユーザデバイスＡから受信したセッション鍵で暗号化されたコンテンツ鍵をセッション鍵で復号し、さらに、ユーザデバイスＢの暗号処理部のメモリに格納されている保存鍵で再暗号化する。ステップＳ１９１２では、コンテンツ使用制限情報（ＵＣＳ（Ｂ））と、保存鍵で暗号化したコンテンツ鍵をフラッシュメモリ等のメモリに格納する。

【０２０３】

ステップＳ１９１３では、ユーザデバイスＡが、ユーザデバイスＢから受領した利用ログに基づいて受領ログを生成してこれをクリアリングセンタに送信する。なお、この受領ログにはユーザデバイスＡの署名が付けられる。クリアリングセンタは署名検証の後、受領ログに基づく決済処理を行なう。なお、先にも延べたように受領ログに基づく決済処理の代わりにコンテンツの二次配布を行なったユーザデバイス、あるいはユーザデバイスの管理をする管理ユーザに対して何らかの優待ポイントを設定する処理を例えばサービスプロバイダにおいて実行する構成とした場合には、受領ログをサービスプロバイダに送信して、サービスプロバイダ側のユーザデータベースにおいてポイント付加処理を実行するようにしてもよい。なお、受領ログはすぐに送信せず、電子マネーを記録管理するメモリ内に保存しておき、適宜、例えば所定数の受領ログを蓄積した後、あるいは所定期間毎等、適当なタイミングで送信処理を実行するようにしてもよい。

【０２０４】

［５．コンテンツ二次配布におけるポイント付加処理］

これまでに説明したように、ユーザデバイス間でのセキュアコンテナを用いたコンテンツの二次配布は、受領ログによってすべて把握管理することが可能であ

る。

【０２０５】

ここでは、受領ログを用いてコンテンツの二次配布を行なったユーザに対して何らかの特典を付与するための優待ポイントを二次配布時のコンテンツ提供者であるユーザデバイスあるいはユーザデバイスを管理する管理ユーザに付与することにより、ユーザ間のコンテンツの二次流通をより活性化させる構成について説明する。

【０２０６】

上述した構成においては、受領ログに含まれる受領情報（図１７参照）に、コンテンツプロバイダの利益額／利益率、サービスプロバイダの利益額／利益率等を記録し、クリアリングセンタがこれらのデータに基づいて、コンテンツ利用料金の決済処理、具体的には、コンテンツプロバイダ、サービスプロバイダ、その他コンテンツ販売店舗、コンテンツ著作者に対してユーザから支払われたコンテンツ利用料金を配分する処理を実行していた。

【０２０７】

先に、図６、図１７を用いて説明した受領情報に二次配布を実行したユーザデバイス、あるいはユーザデバイスを管理する管理ユーザに対するポイント付加情報を設定し、ポイント付加情報を含む受領情報を有する受領ログを、例えばサービスプロバイダに送信する（図１５参照）構成とすることにより、サービスプロバイダが二次配布を実行したユーザデバイスあるいは二次配布を実行したユーザデバイスを管理する管理ユーザに対して何らかの優待ポイントを付加することが可能となる。優待ポイントは、例えば１つのセキュアコンテナの１回の二次配布につき１ポイントとして、ポイント数に応じて、新たなコンテンツの提供価格の割引を行なう。あるいはコンテンツの利用制限の緩和、例えば再生制限回数等を増加して設定する等の処理が可能となる。

【０２０８】

優待ポイントの処理を実行するのは、サービスプロバイダ、クリアリングセンタ、コンテンツプロバイダ、あるいは別のサービス機関によって行なわれてもよいが、ここではサービスプロバイダがポイント処理を行なう例について説明する

。図２０にポイント処理を説明するブロック図を示す。

【０２０９】

図２０において、Ｎｏ．１～Ｎｏ．５は、時系列的な処理順を示している。Ｎｏ．１、Ｎｏ．２の処理は先の図１５において説明した処理と同様であり、Ｎｏ．３の処理がユーザデバイスＡ１５１０からユーザデバイスＢ１５２０へのコンテンツ（セキュアコンテナ）の二次配布において、ユーザデバイスＢ１５２０の発行した利用ログＢ１５５２に基づいてユーザデバイスＡ１５１０が生成した受領ログＢ１５５３をサービスプロバイダ２４０に送付する処理である。

【０２１０】

サービスプロバイダ２４０は、ユーザデバイスＡ１５１０からユーザデバイスＢ１５２０へのコンテンツ（セキュアコンテナ）の二次配布によって生成された受領ログＢ１５５３に基づいて、ポイント付加処理（図２０のＮｏ．４の処理）を実行する。

【０２１１】

サービスプロバイダ２４０のユーザ管理データベース１５３４のデータ構成例を図２１に示す。各データエントリは、図２１に示すようにコンテンツ提供を行なったユーザを示すユーザＩＤ、ユーザデバイスＩＤ、提供したコンテンツを示すコンテンツＩＤ、二次配布に基づく受領ログの識別子としての受領ログＩＤ、二次配布に基づくポイントデータが設定されている。

【０２１２】

サービスプロバイダ２４０は、これらのデータから、ユーザ毎の集計ポイント、あるいはユーザデバイス毎の集計ポイント等を計数し、例えば所定ポイントに達したユーザ、ユーザデバイスに対して特典を与えることが可能となる。特典としては、例えば、次回のコンテンツ価格を割り引いたり、コンテンツ利用制限を緩和したり、あるいは景品サービスを行なうことなどが可能である。

【０２１３】

これらのサービスプロバイダによるポイント付加処理と、前述のクリアリングセンタによるコンテンツ利用料金の決済処理は、それぞれに受領ログを送付することによってそれぞれ実行可能であり、いずれか一方のみの処理、または両者の

処理を並列に実行することも可能である。

【０２１４】

［６．決済処理の具体例］

次に、本発明のコンテンツ取り引きシステムにおける具体的な処理例について図を参照して説明する。

【０２１５】

図２２は、クリアリングセンタと、口座管理機関での決済処理の具体例を示している。図２２において、ユーザデバイス２２１０は、サービスプロバイダまたはユーザデバイスＢ２２２０からコンテンツを購入する。なお、この例においてコンテンツの利用料金は１０００円であるとする。この利用価格、さらに、コンテンツ利用者から徴収した利用料金の配分情報は、コンテンツを格納したセキュアコンテナの価格情報、販売条件に記録されている。

【０２１６】

まず、ユーザデバイスＡ２２１０の電子マネーに対する利用可能な金額の設定処理について説明する。ユーザデバイスＡ２２１０を管理する管理ユーザであるユーザＡは例えば銀行である口座管理機関２２４０に１００，０００円分のユーザＡの口座２２４１を有する。ユーザＡの要求により、口座管理機関２２４０は、電子マネーとして利用可能な金額、１０，０００円を電子マネーを管理するクリアリングセンタ２２３０のユーザＡの電子マネー口座に振り替える。この処理は、電子マネーの電子データ上での決済処理を実行するクリアリングセンタ２２３０に通知され、クリアリングセンタ２２３０は、クリアリングセンタ２２３０内に設置された各ユーザの電子マネー残高を管理するユーザ残高管理サーバのユーザＡの残高を１０，０００円として設定する。この残高設定の後、この設定金額がユーザデバイスＡ２２１０に対して通知される。この通知は、発行ログ２２１１を生成してユーザデバイスＡ２２１０に送信する処理として実行される。なお、この発行ログ送信処理は、相互認証処理、クリアリングセンタの署名処理、ユーザデバイスＡによる署名検証等の一連の処理を行なって実行される。

【０２１７】

この発行ログ２２１１に設定された残高に相当する金額がユーザデバイスＡ２

２１０において電子マネーを使用した支払処理で使用可能となる。これは、クリアリングセンタ２２３０の残高管理データと一致するものとなる。

【０２１８】

ユーザデバイスＡ２２１０は、コンテンツを利用するために電子マネーから１０００円を引出して支払うことになる。ユーザデバイスＡ２２１０は、この支払い処理を利用ログの生成およびコンテンツ提供者に対する利用ログ送付処理として実行する。また、同時に残高情報から１０００を引くため、残高は９，０００円になる。コンテンツ提供者は、サービスプロバイダまたはユーザデバイスＢ２２２０であり、サービスプロバイダまたはユーザデバイスＢ２２２０は、ユーザデバイスＡから受信した利用ログに基づいて、受領ログを生成してクリアリングセンタ２２３０に送付する。

【０２１９】

クリアリングセンタ２２３０は、受領ログに記録された配分情報に従って、決済構成を構築し、これを振り替え要求として口座管理機関２２４０に送信する。ここでの決済処理構成は、コンテンツ受領者（ユーザデバイスＡ２２１０）からコンテンツ提供者（サービスプロバイダまたはユーザデバイスＢ２２２０）にコンテンツ利用料金１０００円を支払う処理とする。

【０２２０】

口座管理機関２２４０は、クリアリングセンタ２２３０から決済処理構成データを受領し、データに従って振替処理を実行する。すなわち、クリアリングセンタの管理するユーザ口座２２４２からコンテンツ利用料金１０００円を引出して、コンテンツ提供者であるサービスプロバイダまたはユーザデバイスＢ２２２０の口座２２４３に１０００円を振り替える処理を実行する。

【０２２１】

これらの一連の処理を実行すると口座管理機関２２４０は、振替確認をクリアリングセンタ２２３０に送信する。クリアリングセンタ２２３０は、振替確認を受信すると、ユーザ残高管理サーバのデータを振り替え処理に応じて更新する。図２２では、ユーザＡの電子マネー残高を１００００円から９０００円に設定する。なお、ユーザ残高管理サーバのデータ中、ユーザＢの残高は０のままである

。これは口座管理機関２２４０のユーザＢの口座は実際の口座であり、電子マネーの残高を示す口座ではないからである。すなわち、クリアリングセンタ口座２２４２内にユーザＢまたはサービスプロバイダの残高がないからである。

【０２２２】

次に、図２３を用いて、ユーザ間でのコンテンツの二次配布（世代間配信または二次配信）により、各ユーザデバイス間でのコンテンツ料金支払いにおいて発生する各ユーザデバイスの電子マネーの残高更新処理例について説明する。

【０２２３】

図２３は、コンテンツプロバイダ２３１０の制作したコンテンツがコンテンツサービスプロバイダ２３２０、ユーザデバイスＡ２３３０を介してユーザデバイスＢ２３４０に流通し、ユーザデバイスＢ２３４０が、コンテンツをユーザデバイスＣ２３５０に配信して、ユーザデバイスＣ２３５０が、ユーザデバイスＢ２３４０に利用料金を支払った場合の処理例である。

【０２２４】

この例において、コンテンツの利用料金は５００円であり、コンテンツを格納したセキュアコンテナの価格情報、販売条件には、図２３の口座管理機関２３７０の［利益配分］の欄に示す配分情報が記録されているものとする。すなわち、コンテンツプロバイダに４００円、サービスプロバイダに１０円、コンテンツ提供ユーザに５０円、クリアリングセンタに４０円の設定がなされている。

【０２２５】

図２３の（１）～（１０）の順に処理が進行する。まず、ユーザデバイスＣ２３５０の管理ユーザは、口座管理機関２３７０のユーザＣ口座に入金処理（図２３の（１）の処理）をするとともに、電子マネーとして利用可能な金額、この場合は１００００円を設定するように要求する。口座管理機関２３７０は、ユーザＣ口座から１００００円をクリアリングセンタ管理口座に振替処理を行ない、これをクリアリングセンタ２３６０に通知する。クリアリングセンタ２３６０は、ユーザ管理サーバと、ユーザ残高管理サーバの各データベースにユーザＣが１００００円の電子マネーを使用可能とする設定を実行し、発行ログをユーザデバイスＣ２３５０に発行（図２３の（２）の処理）する。

【０２２６】

ユーザデバイスＣ２３５０は、ユーザデバイスＢ２３４０からコンテンツ配信を受け（図２３の（３）の処理）、電子マネーによる支払いを行なう。この際、電子マネーの残高をコンテンツ利用料金の５００円分減少させて、ユーザデバイスＣからユーザデバイスＢに対するコンテンツの料金支払いであることが記録された利用ログをユーザデバイスＢ２３４０に発行（図２３の（４）の処理）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【０２２７】

ユーザデバイスＢ２３４０は、ユーザデバイスＣ２３５０から受信した利用ログに基づいて、受領ログを生成してクリアリングセンタ２３６０に送信（図２３の（５）の処理）する。この受領ログは利用ログに記録されたデータを含むものであり、ユーザデバイスＣからユーザデバイスＢに対するコンテンツの料金支払いであること、およびコンテンツ料金配分情報が記録されている

【０２２８】

クリアリングセンタ２３６０は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、コンテンツ料金配分情報に基づく振替構成を構築して、振替構成データを伴う振替要求を口座管理機関２３７０に送信（図２３の（６）の処理）する。

【０２２９】

口座管理機関２３７０は、図２３の口座管理機関２３７０の枠内に記載した通りの［利益配分］情報に従ってそれぞれの口座に対する振替処理を実行（図２３の（７）の処理）する。図には、ユーザＣとユーザＢの電子マネー決済についてのみ記載してあるが、口座管理機関２３７０は、他のコンテンツプロバイダ等の口座に対する振替も実行する。なお、利益配分の情報は、受領ログから抽出してクリアリングセンタ２３６０から口座管理機関２３７０へ送信するようにしてもよい。

【０２３０】

口座管理機関２３７０による振替処理が終了すると、振替確認がクリアリングセンタ２３６０に通知（図２３の（８）の処理）され、クリアリングセンタ２３６０は、自身が管理する電子マネー情報の決済処理、すなわち各ユーザ電子マネー残高の更新処理を実行（図２３の（９）の処理）する。さらに、コンテンツを提供したユーザデバイス２３４０に対してコンテンツの利益配分情報に従った５０円の発行（図２３の（１０）の処理）を行なう。

【０２３１】

なお、一連の処理において、データ通信を実行する各手段は、それぞれ相互認証処理、送信データに対する署名処理、受信データに対する署名確認処理を行なっている。このような一連の処理により、コンテンツのユーザ間における配信において、予めセキュアコンテナに設定された利益配分情報に従った決済処理が実行されることになる。

【０２３２】

上述の図２３の例では、受領ユーザデバイスＣ，２３５０にコンテンツを二次配布したユーザデバイス２３４０が生成した受領ログを直接クリアリングセンタ２３６０に送付する例を示したが、ユーザ間でコンテンツの二次配布（世代間配信または二次配信）を行なったユーザデバイスがクリアリングセンタではなく、サービスプロバイダに受領ログを送付する例を図２４に示す。ユーザデバイスがクリアリングセンタではなく、サービスプロバイダに受領ログを送付することにより、サービスプロバイダにおいて、利益分配処理、ポイント付与の管理等コンテンツ流通に伴う各種の処理を一括して実行することが可能となり、また、クリアリングセンタは電子マネーの発行（発行ログの管理）と受領ログに基づく精算業務のみを実行する構成とすることができる。

【０２３３】

図２４に示す処理構成について説明する。図２４の（１）～（２２）の順に処理が進行する。図２４では、ユーザデバイスＡ２４１０から、ユーザデバイスＢ２４２０にコンテンツが二次配布（世代間配信または二次配信）された例である。まず、ユーザデバイスＢ２４２０がユーザデバイスＡ２４１０にコンテンツを要求（１）する。次に、ユーザデバイスＡ２４１０はコンテンツ（セキュアコン

テナ）をユーザデバイスＢ２４２０に送信（２）する。ユーザデバイスＢ２４２０は、販売条件等を確認して購入処理を実行し、電子マネーによる支払を行なう。この際、電子マネーの残高情報はコンテンツの利用金額に応じて減額（￥２０，０００→￥１９，５００）（３）される。さらにユーザデバイスＢ２４２０は、コンテンツの料金支払いであることが記録された利用ログを生成してユーザデバイスＡに送付（４）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【０２３４】

ユーザデバイスＡ２４１０は、利用ログの署名検証（５）を実行し、利用ログに基づく受領ログを生成して保存（６）し、コンテンツ鍵をユーザデバイスＢ２４２０に送信（７）する。受領ログは利用ログに記録されたデータを含むものであり、ユーザデバイスＣからユーザデバイスＢに対するコンテンツの料金支払いであること、およびコンテンツ料金配分情報が記録されている。ユーザデバイスＡ２４１０は、生成した受領ログをサービスプロバイダ２４３０に送信（８）する。

【０２３５】

受領ログを受信したサービスプロバイダ２４３０は、受領ログの署名を検証して受領ログに記録された利益分配情報、ポイント付与情報に従った処理を実行して、処理データをユーザ管理データベースあるいは利益分配管理サーバに格納する。これらの一連の処理が終了すると、サービスプロバイダ２４３０は受領ログをクリアリングセンタ２４４０に転送（１０）する。

【０２３６】

クリアリングセンタ２４４０は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関２４５０に送信（１１）する。

【０２３７】

口座管理機関２４５０は、クリアリングセンタ２４４０からの振替要求に基づ

いてクリアリングセンタ管理口座２４５１からサービスプロバイダ管理口座２４５２への振替を実行（１２）する。この例では、利益配分情報に基づく利益配分処理は、サービスプロバイダが管理するので、クリアリングセンタ２４４０からの振替要求に基づく処理は、クリアリングセンタ管理口座２４５１からサービスプロバイダ管理口座２４５２への振替処理のみとなる。すなわち、図に示すようにクリアリングセンタ管理口座２４５１が、￥３０，０００から￥２９，５００に変更され、サービスプロバイダの口座２４５２が￥０から￥５００に変更される。口座管理機関２４５０の振替が終了すると、口座管理機関２４５０はクリアリングセンタ２４４０に振替確認を送信（１３）し、クリアリングセンタ２４４０は、振替確認に基づいて電子マネー残高管理サーバ内のユーザデバイスＢ２４２０の管理ユーザであるユーザＢの残高データの更新（１４）を行なう（ユーザＢの残高が￥２０，０００から￥１９，５００に変更される）。この更新により、ユーザデバイスＢ２４２０の電子マネー残高（￥１９，５００）と一致する残高がクリアリングセンタ２４４０の電子マネー残高管理サーバ内のユーザＢの残高データ（￥１９，５００）に記録される。

【０２３８】

次にクリアリングセンタ２４４０は、サービスプロバイダ２４３０にユーザデバイスＢ２４２０からのコンテンツ料金の支払い処理が終了したことを報告（１５）する。サービスプロバイダ２４３０は、クリアリングセンタ２４４０からの報告を受けると、先に受領ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関２４５０に送信（１６）する。口座管理機関２４５０は、サービスプロバイダ２４３０からの配分情報に従ってそれぞれの口座に対する振替処理を実行（１７）する。図２４に示す例では、コンテンツプロバイダの口座２４５３と、クリアリングセンタの口座２４５４にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、振替処理により、クリアリングセンタ管理口座２４５１が￥２９，５００→￥２９，５５０、サービスプロバイダの管理口座２４５２が、￥５００→￥１０、コンテンツプロバイダの口座２４５３が、￥０→￥４００、クリアリングセンタの口座２４５４が、￥０→￥４０に変更される。

【０２３９】

口座管理機関２４５０によるこれらの振替が終了すると、口座管理機関２４５０は、配分処理の終了を示す振替確認をクリアリングセンタ２４４０に送信（１９）する。クリアリングセンタ２４４０は、振替確認を受領すると、クリアリングセンタ２４４０の管理するユーザデバイスＡの電子マネーの残高変更処理（ユーザＡの残高を￥１０，０００から￥１０，０５０に変更）を実行（２０）する。この処理は、先にサービスプロバイダ２４３０から受領した受領ログに基づく処理、すなわち二次配布による利益配分（図の例では￥５０）がユーザデバイスＡ２４１０の管理ユーザであるユーザＡに渡される処理となる。クリアリングセンタ２４４０によるユーザデバイスＡの電子マネーの残高変更処理が終了すると、ユーザデバイスＡに対して利益配分（￥５０）の発行金額を有する新たな発行ログを送信（２１）し、ユーザデバイスＡ２４１０は発行ログに基づいて電子マネーの残高を変更（２２）（残高を￥１０，０００から￥１０，０５０に変更）する。

【０２４０】

なお、図の（２１）で送付する発行ログは、前述した発行ログの追加発行処理と同様の処理として、すでにユーザデバイスＡ２４１０に対して発行済みの「発行ログ－ｏｌｄ」と電子マネー残高データの送信をクリアリングセンタ２４４０側から要求し、ユーザＡに対する利益額と、ユーザから受信した「発行ログ－ｏｌｄ」に基づく電子マネー使用可能残高との合計を新たな発行ログである「発行ログ－ｎｅｗ」の発行金額として設定して新たな発行ログ「発行ログ－ｎｅｗ」をユーザデバイスＡに送信する構成としてもよい。この場合、「発行ログ－ｏｌｄ」はクリアリングセンタ２４４０において無効化される。

【０２４１】

次に、図２５を用いて、各種ログを用いたコンテンツ配信における決済処理の処理例について説明する。図２５はコンテンツ流通における決済処理の管理の中心がサービスプロバイダであるローカル管理方式の例である。

【０２４２】

図２５に示す番号（１）～（１８）の順に処理が進行する。この例では、サー

ビスプロバイダ２５２０からユーザデバイスＡ２５１０がコンテンツを購入する場合の処理例である。

【０２４３】

まず、ユーザデバイスＡ２５１０は、電子マネーによる支払処理を可能とするため、クリアリングセンタ２５３０のユーザ管理サーバへの登録および電子マネー残高管理サーバの残高を設定する処理をクリアリングセンタ２５３０に対して入金命令（１）として要求する（電子マネー：￥０→￥１０，０００）。クリアリングセンタ２５３０は要求に従って口座管理機関２５４０に対してユーザＡの口座２５４１からクリアリングセンタ管理口座２５４２への振替を要求し、口座管理機関２５４０は要求に従って振り替え処理を実行（２）する（ユーザＡの口座２５４１：￥１０，０００→￥９０，０００、クリアリングセンタの口座２５４２：￥０→￥１０，０００）。振替処理が終了すると確認応答がクリアリングセンタ２５３０に対してなされ、応答に応じて、クリアリングセンタ２５３０は、電子マネー残高管理サーバのユーザＡの残高を入金処理金額に応じて更新（３）（ユーザＡ２５１０の電子マネー：￥０→￥１０，０００）し、その金額を発行金額として設定した発行ログをユーザデバイスＡ２５１０に送信（４）する。

【０２４４】

次に、ユーザデバイスＡ２５１０は、サービスプロバイダ２５２０にコンテンツを要求（５）する。次に、サービスプロバイダ２５２０はコンテンツ（セキュアコンテナ）をユーザデバイスＡ２５１０に送信（６）する。ユーザデバイスＡ２５１０は、販売条件等を確認して購入処理を実行し、電子マネーによる支払い処理としての電子マネー残高変更（７）を実行（￥１０，０００→￥９，５００）し、コンテンツの料金支払いであることが記録された利用ログを生成してサービスプロバイダ２５２０に送付（８）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【０２４５】

サービスプロバイダ２５２０は、利用ログの署名検証を実行（９）し、利用ログに基づくコンテンツ料金配分情報を取得して、受領ログを生成・保存（１０）して、コンテンツ鍵をユーザデバイスＡ２５１０に送信（１１）する。その後、

決済時に受領ログをクリアリングセンタ２５３０に送信（１２）する。

【０２４６】

クリアリングセンタ２５３０は、受領ログの格納データとユーザ管理サーバのユーザデータとの照合処理を実行して、センタの管理するユーザによる決済要求であることを確認して、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関２５４０に送信（１３）する。

【０２４７】

口座管理機関２５４０は、クリアリングセンタ２５３０からの振替要求に基づいてクリアリングセンタ管理口座２５４２からサービスプロバイダ管理口座２５４３への振替を実行（１４）する（サービスプロバイダ管理口座２５４３：￥０→￥５００）。この例では、利益配分情報に基づく利益配分処理は、サービスプロバイダ２５２０が管理するので、クリアリングセンタ２５３０からの振替要求に基づく処理は、クリアリングセンタ管理口座２５４２からサービスプロバイダ管理口座２５４３への振替処理のみとなる。口座管理機関２５４０の振替が終了すると、口座管理機関２５４０はクリアリングセンタ２５３０に振替確認を送信（１５）し、クリアリングセンタ２５３０は、振替確認に基づいて電子マネー残高管理サーバ内のユーザＡ（ユーザデバイスＡ２５１０の管理ユーザ）の残高データの更新（１６）（￥１０，０００→￥９，５００）を行なう。

【０２４８】

次にクリアリングセンタ２５３０は、サービスプロバイダ２５２０にユーザデバイスＡ２５１０からのコンテンツ料金の支払い処理が終了したことを振替確認として報告（１７）する。サービスプロバイダ２５２０は、クリアリングセンタ２５３０からの報告を受けると、先に利用ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関２５４０に送信する。口座管理機関２５４０は、サービスプロバイダ２５２０からの配分情報に従ってそれぞれの口座に対する振替処理を実行（１８）する。図２５に示す例では、コンテンツプロバイダの口座２５４４と、クリアリングセンタの口座２５４５にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、サービスプロバイダ管理口座

２５４３：￥５００→￥６０、コンテンツプロバイダの口座２５４４：￥０→￥４００、クリアリングセンタの口座２５４５：￥０→￥４０の振替がなされる。

【０２４９】

この図２５の例は、サービスプロバイダが利益分配、ポイント管理等のコンテンツ流通に伴う各処理を実行し、クリアリングセンタは電子マネーの残高管理が主業務となる。

【０２５０】

次に、図２６を用いて、ユーザデバイスにおいて残高管理を実行せず、クリアリングセンタが電子マネーの残高管理を行なうクリアリングセンタ管理方式の処理例を説明する。（１）～（１５）の順に処理が進行する。この例では、サービスプロバイダ２６２０からユーザデバイスＡ２６１０がコンテンツを購入する場合の処理例である。

【０２５１】

まず、ユーザデバイスＡ２６１０は、電子マネーによる支払処理を可能とするため、クリアリングセンタ２６３０のユーザ管理サーバへの登録および電子マネー残高管理サーバの残高を設定する処理をクリアリングセンタ２６３０に対して入金命令（１）として要求する。クリアリングセンタ２６３０は要求に従って口座管理機関２６４０に対してユーザデバイスＡ２６１０の管理ユーザであるユーザＡの口座２６４１からクリアリングセンタ管理口座２６４２への振替を要求し、口座管理機関２６４０は要求に従って振り替え処理を実行（２）する。すなわち、ユーザＡの口座２６４１：￥１００，０００→￥９０，０００、クリアリングセンタ管理口座２６４２：￥０→￥１０，０００の振替が実行される。振替処理が終了すると確認応答がクリアリングセンタ２６３０に対してなされ。応答に応じて、クリアリングセンタ２６３０は、電子マネー残高管理サーバのユーザＡの残高を入金処理金額に応じて更新（３）（￥０→￥１０，０００）する。

【０２５２】

このセンタ管理方式では、ユーザデバイスＡ２６１０は、クリアリングセンタ２６３０に入金命令を送信するとともにサービスプロバイダ２６２０にコンテンツを要求（４）することができる。先の図２５の例では、ユーザデバイス側におい

て電子マネーの残高チェックを実行シテコンテンツの購入処理を実行していたが、本例では、クリアリングセンタ側で電子マネー残高を更新して、その報告を受けたサービスプロバイダ２６２０が、その報告後、ユーザデバイスＡに対してコンテンツ鍵を送信する方式となっている。

【０２５３】

ユーザデバイスＡ２６１０がサービスプロバイダ２６２０にコンテンツを要求すると、サービスプロバイダ２６２０はコンテンツ（セキュアコンテナ）をユーザデバイスＡ２６１０に送信（５）する。ユーザデバイスＡ２６１０は、販売条件等を確認して購入処理を実行し、電子マネーによる支払い、コンテンツの料金支払いであることが記録された利用ログを生成してサービスプロバイダ２６２０に送付（６）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【０２５４】

サービスプロバイダ２６２０は、利用ログの署名検証を実行し、利用ログに基づくコンテンツ料金配分情報を取得して、受領ログを生成してクリアリングセンタ２６３０に送信（７）する。

【０２５５】

クリアリングセンタ２６３０は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、電子マネー残高管理サーバの残高確認（８）を行い、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関２６４０に送信（９）する。

【０２５６】

口座管理機関２６４０は、クリアリングセンタ２６３０からの振替要求に基づいてクリアリングセンタ管理口座２６４２からサービスプロバイダ管理口座２６４３への振替を実行（１０）する（クリアリングセンタ管理口座２６４２：￥１０，０００→￥９，５００、サービスプロバイダ管理口座２６４３：￥０→￥５００）。この例においても、利益配分情報に基づく利益配分処理は、サービスプ

ロバイダ２６２０が管理するので、クリアリングセンタ２６３０からの振替要求に基づく処理は、クリアリングセンタ管理口座２６４２からサービスプロバイダの口座２６４３への振替処理のみとなる。口座管理機関２６４０の振替が終了すると、口座管理機関２６４０はクリアリングセンタ２６３０に振替確認を送信（１１）し、クリアリングセンタ２６３０は、振替確認に基づいて電子マネー残高管理サーバ内のユーザＡの残高データの更新（￥１０，０００→￥９，５００）（１２）を行なう。

【０２５７】

次にクリアリングセンタ２６３０は、サービスプロバイダ２６２０にユーザデバイスＡ２６１０からのコンテンツ料金の支払い処理が終了したことを振替確認送信（１３）する。サービスプロバイダ２６２０は、クリアリングセンタ２６３０からの振替確認を受けると、コンテンツ鍵をユーザデバイスＡ２６１０に送信（１４）する。さらに、サービスプロバイダ２６２０は、先に利用ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関２６４０に送信する。口座管理機関２６４０は、サービスプロバイダ２６２０からの配分情報に従ってそれぞれの口座に対する振替処理を実行（１５）する。図２６に示す例では、コンテンツプロバイダの口座２６４４と、クリアリングセンタの口座２６４５にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、サービスプロバイダの口座２６４３：￥５００→￥６０、コンテンツプロバイダの口座２６４４：￥０→￥４００、クリアリングセンタの口座２６４５：￥０→￥４０の各振替がなされる。

【０２５８】

本例においては、ユーザデバイスＡ２６１０は、電子マネーの残高確認が不要であり、クリアリングセンタ２６３０において、電子マネー残高管理サーバ内のユーザ残高が確認され、口座管理機関２６４０において、ユーザＡからのコンテンツ利用料金振替が行なわれて、クリアリングセンタ２６３０内で管理する電子マネー残高の更新がなされ、これらの処理が完結したことをサービスプロバイダ２６２０に報告されて始めて、コンテンツ鍵がユーザデバイスＡ２６１０に送信されることになる。この処理構成によれば、クリアリングセンタ２６３０におい

て未決済分のコンテンツ料金の発生を防止することができる。なお、手数料を減らすため、実際の振替処理は一括して行ない、クリアリングセンタ２６３０内のデータのみ変更して後に振替処理を行なう構成としてもよい。

【０２５９】

［７．ログを利用したユーザ管理］

先に説明したように、本発明のコンテンツ取り引きシステムおよびコンテンツ取り引き方法においては、発行ログ、利用ログ、受領ログ等が各デバイス、機関において流通することになる。各ログには図６で説明したように、様々な情報が格納されている。ここでは、これらの情報を利用したユーザ管理構成について説明する。

【０２６０】

（７－１）ユーザの利用料金の管理

図６を用いて説明した各ログの構成において明らかなように、コンテンツを購入しようとするユーザが生成してサービスプロバイダに対して送信する利用ログには、利用金額が情報として格納されている。ここでは、この利用ログに記録される利用金額情報を利用して高額な料金の支払をチェックする構成を説明する。

【０２６１】

図２７に利用料金チェック処理フローを示す。図２７のフローにしたがって説明する。ステップＳ２７０１において、ユーザが生成した利用ログがサービスプロバイダに送信される。ステップＳ２７０２において、サービスプロバイダは受領した利用ログ中の利用金額を確認し、予め定めた閾値との比較処理を実行する。この閾値は、例えばすべてのユーザに対して共通の閾値でもよいし、あるいはユーザの年齢、利用状況等に基づいてサービスプロバイダが独自に設定した閾値でもよい。サービスプロバイダはこれらの閾値を設定したユーザ管理用のデータを保有する。

【０２６２】

ステップＳ２７０３において要検査の判定がなされると、サービスプロバイダは、ステップＳ２７０４において利用ログから発行ログを取り出して、取り出した発行ログをクリアリングセンタに送信する。ステップＳ２７０５において、ク

リアリングセンタは、サービスプロバイダから受領した発行ログに基づいて、クリアリングセンタ内の電子マネー残高管理サーバのユーザ残高をチェックし、ステップＳ２７０６においてクリアリングセンタは残高チェックデータをサービスプロバイダに送信する。サービプロバイダはチェックデータに基づいて問題なし（ステップＳ２７０７においてＹｅｓ）と判定された場合は、正当なコンテンツ購入処理と判定し、ユーザデバイスに対するコンテンツ鍵送信等の通常処理（ステップＳ２７０８）に移行する。一方、コンテツ利用料金の回収が困難になるおそれがある等、問題あり（ステップＳ２７０７においてＮｏ）と判定された場合は、ユーザデバイスに対してコンテンツ購入の拒否応答を行ないコンテンツ鍵の送信を中止（ステップＳ２７０９）する。

【０２６３】

この処理により、コンテンツの不正取引、あるいは未成年者による高額商品の取引等を未然に防止することが可能となる。なお、これらの利用金額チェックはクリアリングセンタがみずから実行する構成として、問題ありと判定された場合にクリアリングセンタからサービスプロバイダに例えばユーザ照会処理を実行するように要求する構成としてもよい。

【０２６４】

さらに、ユーザデバイス側において、ユーザデバイス固有の利用金額上限値としての閾値を設定し、設定した閾値データをメモリに格納し、コンテンツ利用に伴う利用ログの生成の際に閾値データを参照して、利用ログに閾値を超える利用金額が設定される場合は、閾値を超える利用料金の設定であることまたはクリアリングセンタによるチェック処理が必要であることを示す識別データ（識別ビット）を利用ログに付加する構成としてもよい。識別データが付加された利用ログを受領したサービスプロバイダは、識別データに基づいてクリアリングセンタに対するユーザの残高チェック処理を要求する。本構成によれば、サービスプロバイダ側でユーザの閾値データを保有する必要がなく、さらにユーザ毎に任意の閾値を設定することが可能となる。

【０２６５】

（７－２）発行ログの利用期限管理

前述の本発明の説明から明らかなようにコンテンツを購入しようとするユーザは、クリアリングセンタから発行ログを受領する。発行ログには図６に示したように、有効期限が設定されている。ここでは、この有効期限に基づく管理について説明する。

【０２６６】

クリアリングセンタは、ユーザ管理サーバに発行ログを発行したユーザとその発行ログ情報を対応付けたデータを保有している。発行ログには発行金額、有効期限が設定され、発行ログを受領したユーザデバイスは、その発行ログに設定された金額および有効期限内で発行ログに基づいて電子マネーによる支払い処理が可能となる。

【０２６７】

クリアリングセンタでは、例えば未成年者には小額の発行金額を上限として設定したり、取り引き回数に応じて高額の発行金額を設定する等、ユーザの信用度に基づく発行金額の設定を行なうことができる。さらに、高額な発行金額を設定した発行ログは有効期限を長く設定し、低額の発行金額を設定した発行ログは有効期限を短くする等、各発行ログに応じた有効期限設定が可能となる。

【０２６８】

クリアリングセンタは、ユーザ管理サーバにおいてすべての発行ログ情報を管理しているとともに、電子マネー残高管理サーバにおいて各ユーザの電子マネー残高を管理しているので、クリアリングセンタは、これらの各データに基づいて定期的な監査処理を実行し、有効期限の迫った発行ログを有するユーザに対して、発行ログの有効期限を更新した新たな発行ログの発行要求を促すメッセージを送信する等の処理が可能となる。

【０２６９】

クリアリングセンタによる発行ログの有効期限管理処理のフローを図２８に示す。ステップＳ２８０１において、クリアリングセンタは、ユーザ管理サーバ、電子マネー残高管理サーバとのデータチェックを実行し、ユーザ管理サーバの格納データに基づいて有効期限が迫っている発行ログを抽出する。このチェック処理は、例えば１ヶ月毎に定期的に実行して、残り有効期限が２ヶ月以内である発

行ログを検索する処理として設定する。

【０２７０】

クリアリングセンタは抽出された発行ログに基づいて発行ログ情報に記録されたユーザデバイス識別子に基づいてユーザデバイスを特定（ステップＳ２８０２）し、そのユーザデバイスに対して有効期限の迫った発行ログがあることを示すメッセージを送信（ステップＳ２８０３）する。ユーザデバイスは、メッセージを受信し、発行ログの更新要求を実行する（ステップＳ２８０４でＹｅｓ）と、クリアリングセンタは更新要求に基づいて、新たな有効期限を持つ更新された発行ログを生成してユーザデバイスに送信（ステップＳ２８０５、Ｓ２８０６）する。ユーザデバイスが、メッセージを受信後、有効期間内に発行ログの更新要求を実行しない（ステップＳ２８０４でＮｏ）場合は、有効期間経過後、発行ログの利用期間が経過したことと再発行処理が必要であることを知らせるメッセージをユーザデバイスに送信（ステップＳ２８０７）し、クリアリングセンタは、その後のユーザデバイスからの再発行要求があった場合（ステップＳ２８０８でＹｅｓ）は要求に基づいて発行ログの再発行処理を行ない（ステップＳ２８０９）、再発行ログをユーザデバイスに送信（ステップＳ２８１０）する。

【０２７１】

このように、クリアリングセンタによって発行ログの管理を行なう構成とすることにより、不正な発行ログの流通、使用を防止することができる。さらに、発行ログの有効期限チェックの際に、クリアリングセンタ電子マネー残高管理サーバの残高を併せてチェックすることにより、利用、回収済みの電子マネー金額と未回収分の電子マネーの集計が可能となる。

【０２７２】

また、クリアリングセンタは、電子マネー残高管理サーバの定期的なチェックを実行して、電子マネー残高が小額となったユーザデバイスに対して、その旨のメッセージを送信したり、あるいは、残金額をデータとして送信するように構成してもよい。

【０２７３】

さらに、ユーザデバイス側において、電子マネーの利用時に発行ログの有効期

限のチェック処理を実行し、有効期限が過ぎていた場合には、利用ログの生成処理前にクリアリングセンタに対して発行ログの更新あるいは再発行処理の要求を実行して新たな発行ログの取得を行い、その後に新たな有効期限の設定された新規発行ログに基づく利用ログの生成処理を実行する構成としてもよい。

【０２７４】

なお、一連の処理において、データ通信を実行するユーザデバイス、クリアリングセンタ、サービスプロバイダ各手段は、それぞれ相互認証処理、送信データに対する署名処理、受信データに対する署名確認処理を行ない、不正なデータ流出が行われない構成とする。

【０２７５】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２７６】

【発明の効果】

上述したように、本発明のコンテンツ取り引きシステムおよびコンテンツ取り引き方法に従えば、コンテンツプロバイダ、コンテンツ販売会社等は、クレジットカード、あるいは銀行口座指定によるオンラインでの決済システムを構築する必要がなく、また、ユーザ間におけるコンテンツ取り引き処理における決済処理、あるいはポイント付加処理が、予め設定した配分情報に基づいて実行されることになる。また、１つのコンテンツの複数ユーザ間での譲渡が可能となり、同一コンテンツの利用毎の利用管理が可能となる。

【図面の簡単な説明】

【図１】

従来の超流通システムの構成を説明するブロック図である。

【図２】

本発明のコンテンツ取り引きシステムのシステム概要を説明するブロック図で

ある。

【図３】

本発明のコンテンツ取り引きシステムにおいてユーザデバイスの構成例を示すブロック図である。

【図４】

本発明のコンテンツ取り引きシステムにおけるコンテンツの流通、ログ情報の流通形態について説明するブロック図である。

【図５】

本発明のコンテンツ取り引きシステムにおける相互認証処理において使用される公開鍵証明書の構成について説明する図である。

【図６】

本発明のコンテンツ取り引きシステムにおいて使用される発行ログ、利用ログ、受領ログ構成を説明する図である。

【図７】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名生成処理について説明する図である。

【図８】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名生成処理について説明する図である。

【図９】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名検証処理について説明する図である。

【図１０】

本発明のコンテンツ取り引きシステムにおいて適用可能な相互認証処理について説明する図である。

【図１１】

本発明のコンテンツ取り引きシステムにおいて適用可能な相互認証処理について説明する図である。

【図１２】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通において使用されるセキュアコンテナの構成を説明する図である。

【図１３】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナに含まれる販売条件情報（ＵＣＰ）について説明する図である。

【図１４】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナに含まれる価格情報について説明する図である。

【図１５】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナの流通とログ情報に基づく決済処理構成を説明する図である。

【図１６】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナの流通において、ユーザデバイスに記録される使用制御情報（ＵＣＳ）について説明する図である。

【図１７】

本発明のコンテンツ取り引きシステムにおいて発行される受領ログに含まれる受領情報の構成例を説明する図である。

【図１８】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通における処理を説明する図である。

【図１９】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通における処理フローを説明する図である。

【図２０】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通におけるポイント付加処理を説明する図である。

【図２１】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバ

イス間での流通におけるポイント付加処理に使用されるデータベース構成例を説明する図である。

【図２２】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例を説明する図である。

【図２３】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス間のコンテンツ流通による決済処理の具体例（その１）を説明する図である。

【図２４】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス間のコンテンツ流通による決済処理の具体例(その２)を説明する図である。

【図２５】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例（ローカル管理方式）を説明する図である。

【図２６】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例（クリアリングセンタ管理方式）を説明する図である。

【図２７】

本発明のコンテンツ取り引きシステムにおける利用ログの利用金額による決済管理処理フローを説明する図である。

【図２８】

本発明のコンテンツ取り引きシステムにおける発行ログの有効期限による発行ログ管理フローを説明する図である。

【符号の説明】

２２０　ユーザデバイス

２２１　電子マネー

２２２　発行ログ

２４０　サービスプロバイダ

２５１　発行ログ

２５２　利用ログ

２５３　受領ログ

２６０　クリアリングセンタ

２８０　口座管理機関

２８１　ユーザ口座

２８２　サービスプロバイダ口座

２８３　クリアリングセンタ管理口座

３００　ユーザデバイス

３０１　制御部

３０２　暗号処理部

３０３　記録デバイスコントローラ

３０４　読み取り部

３０５　通信部

３０６　制御部

３０７　内部メモリ

３０８　暗号／復号化部

３１０　電子マネー

３１１　制御部

３１２　暗号処理部

３１３　メモリ

３２１　メインＣＰＵ

３２２　ＲＡＭ

３２３　ＲＯＭ

３２４　入力インタフェース

３２６　ＰＩＯ

３２７　ＳＩＯ

３５０　記録デバイス

３５１　暗号処理部

３５２　外部メモリ

３６０　メディア

３７０　通信手段

４１０　公開鍵証明書発行局（ＩＡ）

１２００　セキュアコンテナ

１２０１　コンテンツ

１２０２　価格情報

１２０３　販売情報（ＵＣＰ）

１２０４　電子署名

１３０１　ＵＣＰ世代管理情報

１３０２　二次配信可能回数

１５１０　ユーザデバイスＡ

１５２０　ユーザデバイスＢ

１５１１，１５２１　電子マネー

１５３１　発行ログＡ

１５３２　利用ログＡ

１５３３　受領ログＡ

１５５１　発行ログＢ

１５５２　利用ログＢ

１５５３　受領ログＢ

１５７０　ユーザデバイスＣ

１６０１　ＵＣＳ世代管理情報

１７０１　配分情報

１７０２　ＵＣＰ世代管理情報

１８１０　サービスプロバイダ

１８１１　制御部

１８１２　コンテンツデータベース

１８１３　ユーザ情報データベース

１８１４　暗号処理部

１８１５　通信部

１８２０　ユーザデバイスＡ

１８３０　ユーザデバイスＢ

１８２１，１８３１　制御部

１８２２，１８３２　暗号処理部

１８２４，１８３４　メモリ

１８２５，１８３５　記憶部

１８２６，１８３６　データ再生部

１８２７，１８３７　通信部

１８２８，１８３８　電子マネー

１８４０　クリアリングセンタ

１８４１　制御部

１８４２　データベース

１８４４　暗号処理部

１８４５　通信部

２２１０　ユーザデバイスＡ

２２１１　発行ログ

２２２０　サービスプロバイダまたはユーザデバイスＢ

２２３０　クリアリングセンタ

２２４０　口座管理機関

２２４１　ユーザＡ口座

２２４２　クリアリングセンタ口座

２２４３　サービスプロバイダ、ユーザＢ口座

２３１０　コンテンツプロバイダ

２３２０　サービスプロバイダ

２３３０　ユーザデバイスＡ

２３４０　ユーザデバイスＢ

２３５０　ユーザデバイスＣ

２３６０　クリアリングセンタ

２３７０　口座管理機関

２４１０，２４２０，２５１０，２６１０　ユーザデバイス

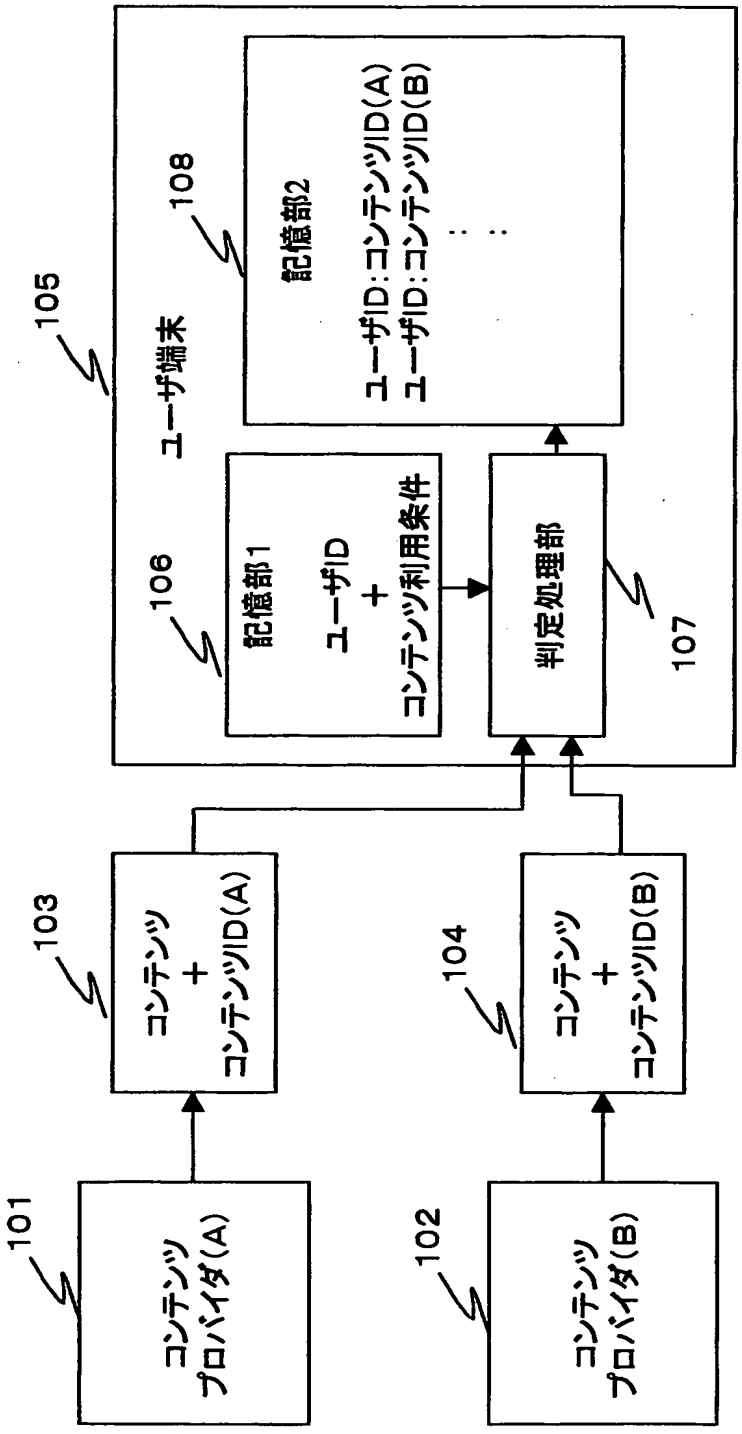
２４３０，２５２０，２６２０　サービスプロバイダ

２４４０，２５３０，２６３０　クリアリングセンタ

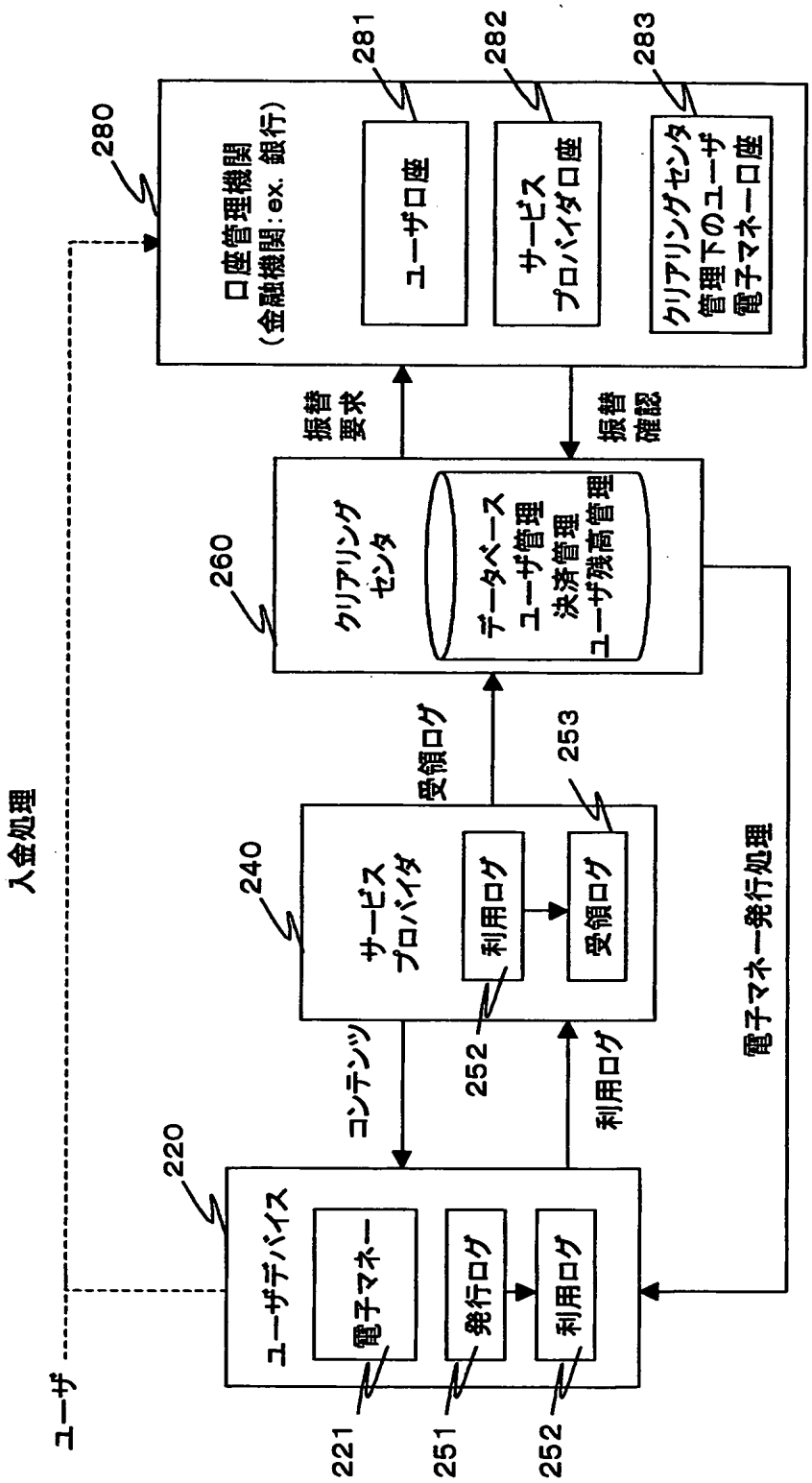
２４５０，２５４０，２６４０　口座管理機関

【書類名】　　図面

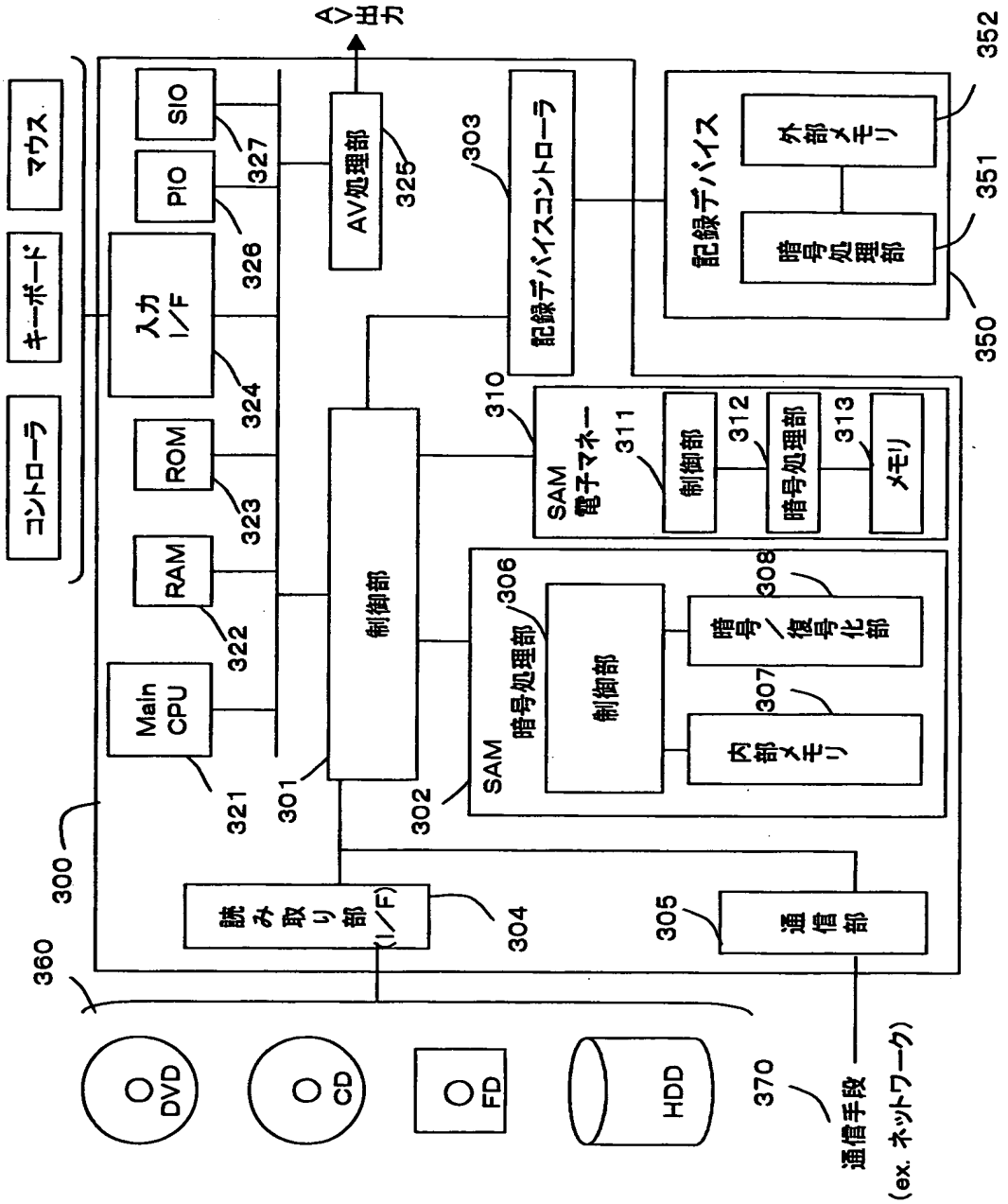
【図１】


101
コンテンツ
プロバイダ(A)
102
コンテンツ
プロバイダ(B)
103
コンテンツ
＋
コンテンツID(A)
104
コンテンツ
＋
コンテンツID(B)
105
ユーザ端末
106
記憶部1
ユーザID
＋
コンテンツ利用条件
107
判定処理部
108
記憶部2
ユーザID:コンテンツID(A)
ユーザID:コンテンツID(B)
：　：

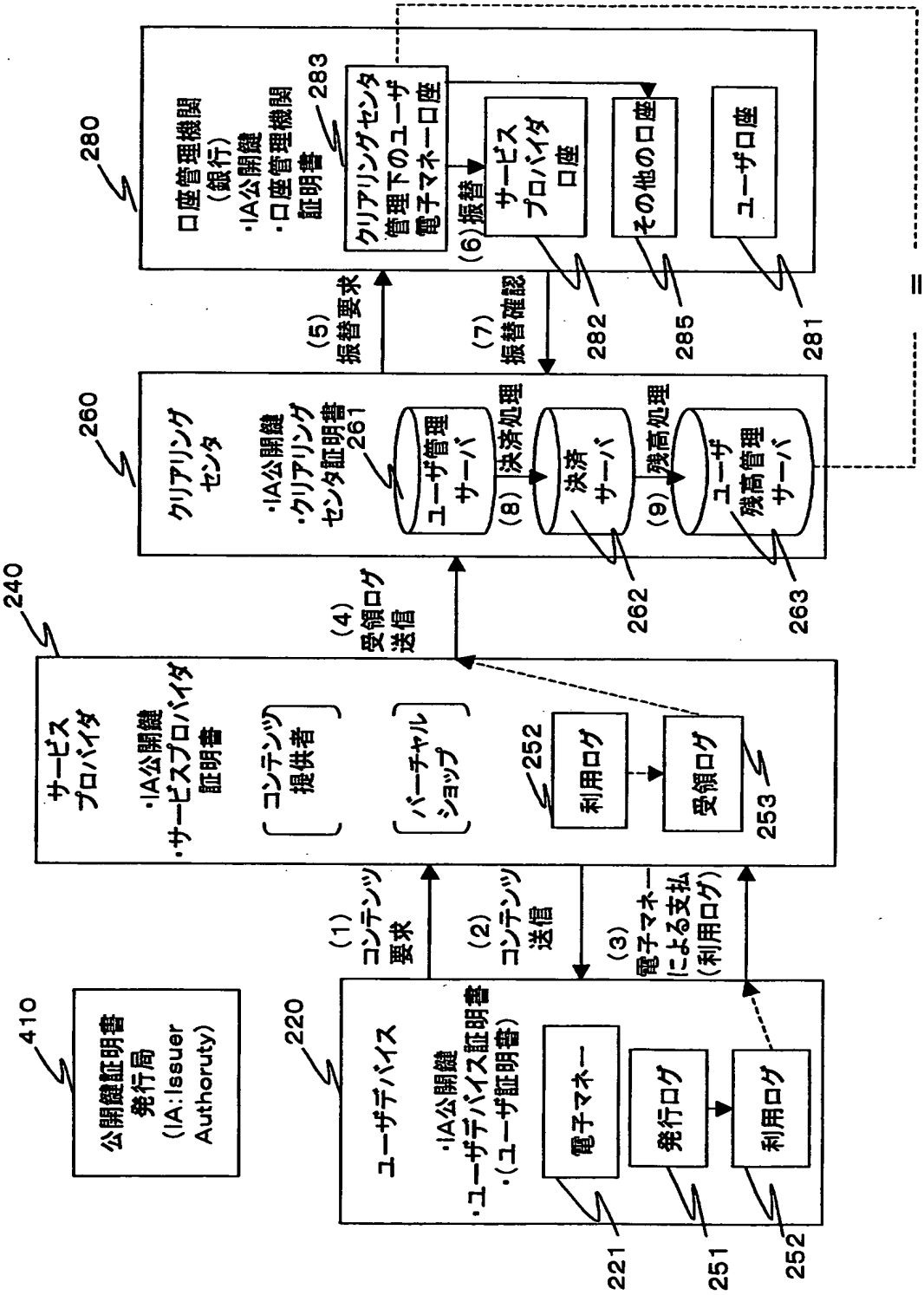
【図２】


280
口座管理機関
（金融機関：ex. 銀行）
281
ユーザ口座
282
サービス
プロバイダ口座
283
クリアリングセンタ
管理下のユーザ
電子マネー口座
振替
要求
振替
確認
260
クリアリング
センタ
データベース
ユーザ管理
決済管理
ユーザ残高管理
受領ログ
253
240
サービス
プロバイダ
利用ログ
受領ログ
252
コンテンツ
利用ログ
入金処理
電子マネー発行処理
220
ユーザデバイス
電子マネー
発行ログ
利用ログ
221
251
252
ユーザ

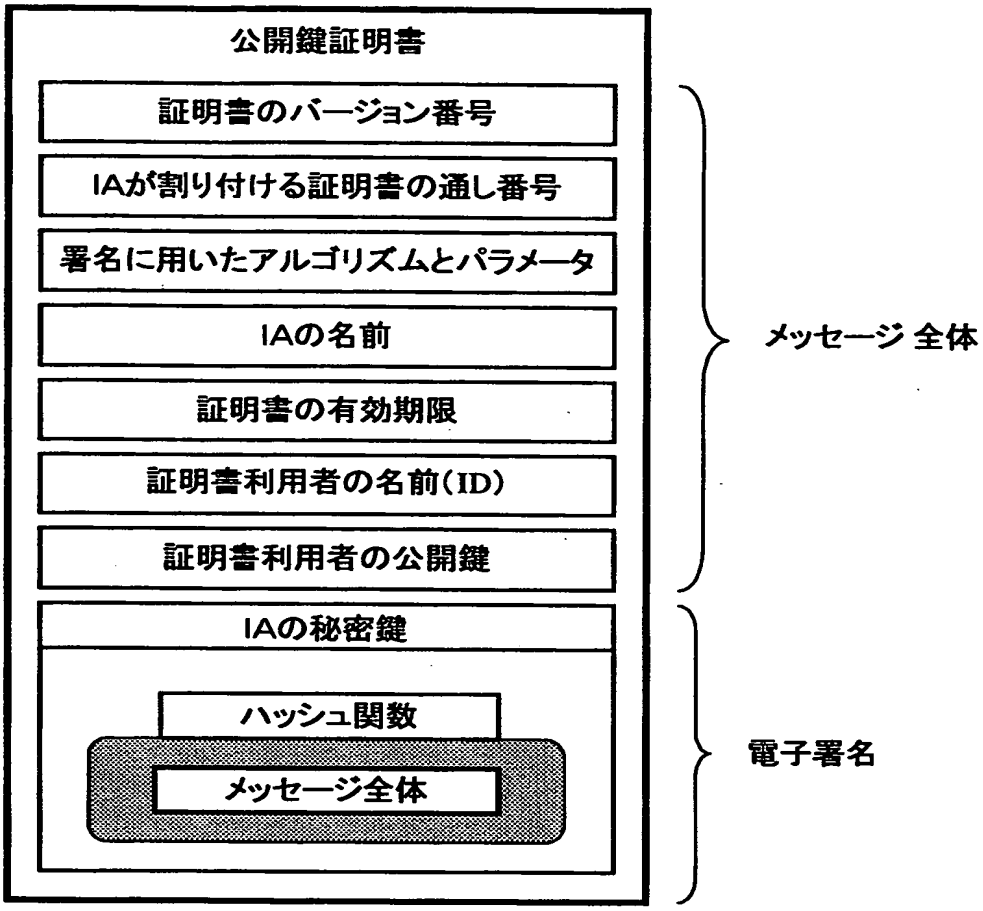
【図３】


A/V出力
352
351
350
マウス
キーボード
コントローラ
入力 I/F
SIO
PIO
ROM
RAM
Main CPU
327
326
324
323
322
321
AV処理部
325
303
記録デバイスコントローラ
記録デバイス
外部メモリ
暗号処理部
310
SAM 電子マネー
311
制御部
312
暗号処理部
313
メモリ
制御部
301
300
302
SAM 暗号処理部
306
制御部
暗号／復号化部
308
内部メモリ
307
読み取り部 (I/F)
304
305
通信部
360
DVD
CD
FD
HDD
370
通信手段
(ex. ネットワーク)

【図４】

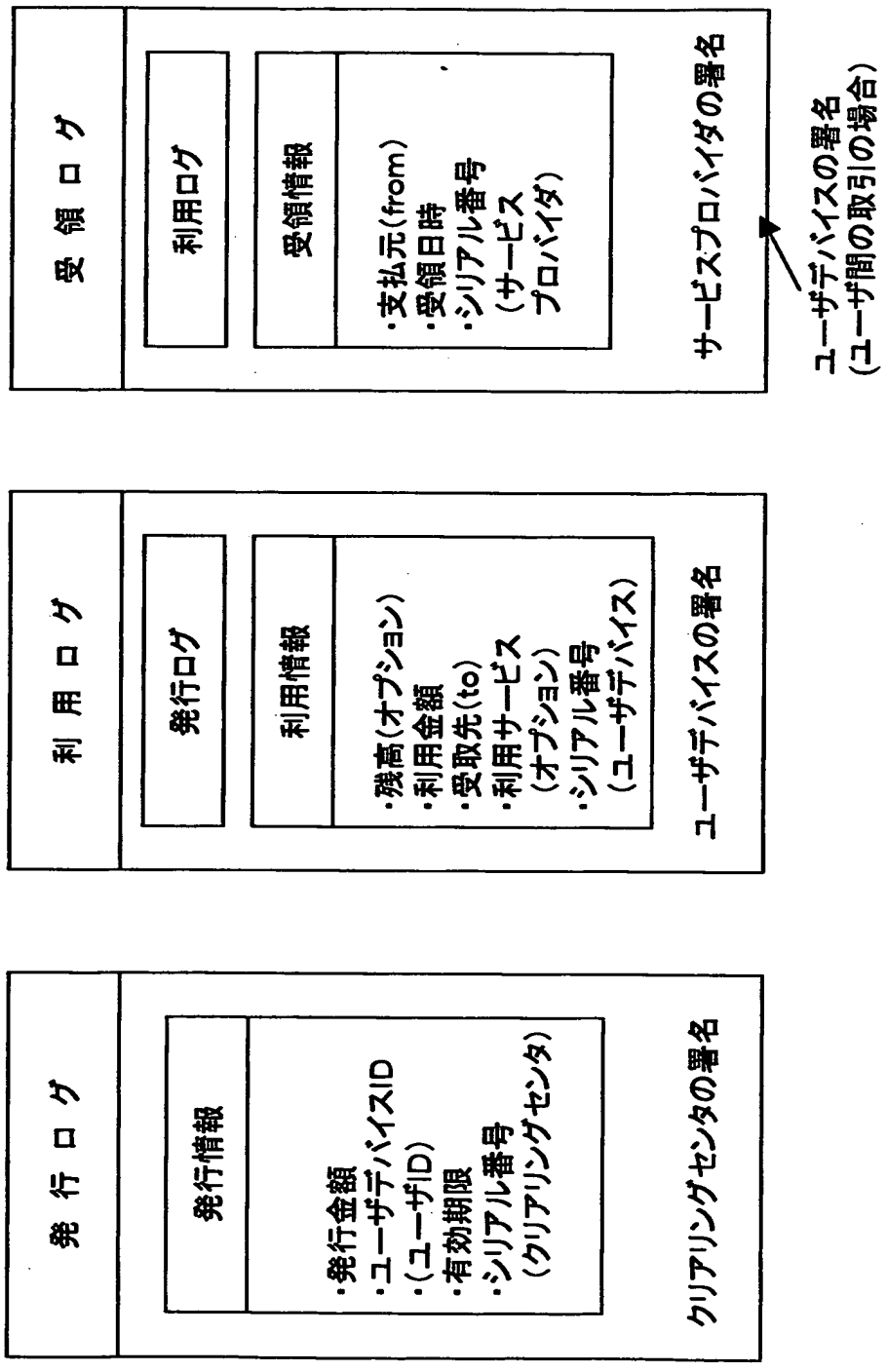

公開鍵証明書
発行局
(IA:Issuer
Authoruty)
410
ユーザデバイス
・IA公開鍵
・ユーザデバイス証明書
・(ユーザ証明書)
220
電子マネー
221
発行ログ
251
利用ログ
252
(1)
コンテンツ
要求
(2)
コンテンツ
送信
(3)
電子マネー
による支払
(利用ログ)
サービス
プロバイダ
・IA公開鍵
・サービスプロバイダ
証明書
240
コンテンツ
提供者
バーチャル
ショップ
252
利用ログ
受領ログ
253
(4)
受領ログ
送信
クリアリング
センタ
・IA公開鍵
・クリアリング
センタ証明書
261
260
ユーザ管理
サーバ
(8)
決済処理
決済
サーバ
262
(9)
残高処理
ユーザ
残高管理
サーバ
263
(5)
振替要求
(7)
振替確認
口座管理機関
(銀行)
・IA公開鍵
・口座管理機関
証明書
280
クリアリングセンタ
管理下のユーザ
電子マネー口座
283
(6)振替
サービス
プロバイダ
口座
282
その他の口座
285
ユーザ口座
281

【図５】

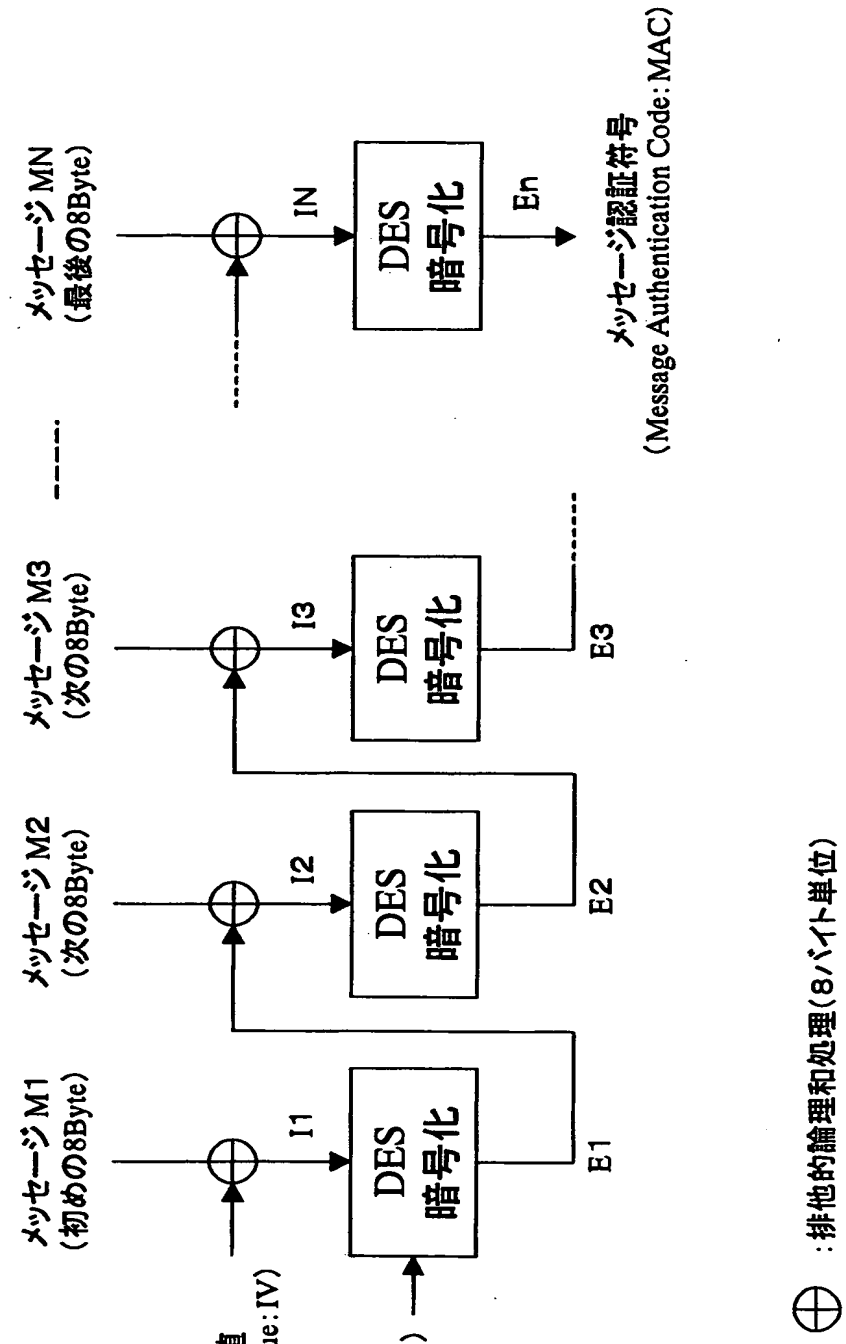

公開鍵証明書
証明書のバージョン番号
IAが割り付ける証明書の通し番号
署名に用いたアルゴリズムとパラメータ
IAの名前
証明書の有効期限
証明書利用者の名前(ID)
証明書利用者の公開鍵
IAの秘密鍵
ハッシュ関数
メッセージ全体
メッセージ 全体
電子署名

公開鍵証明書

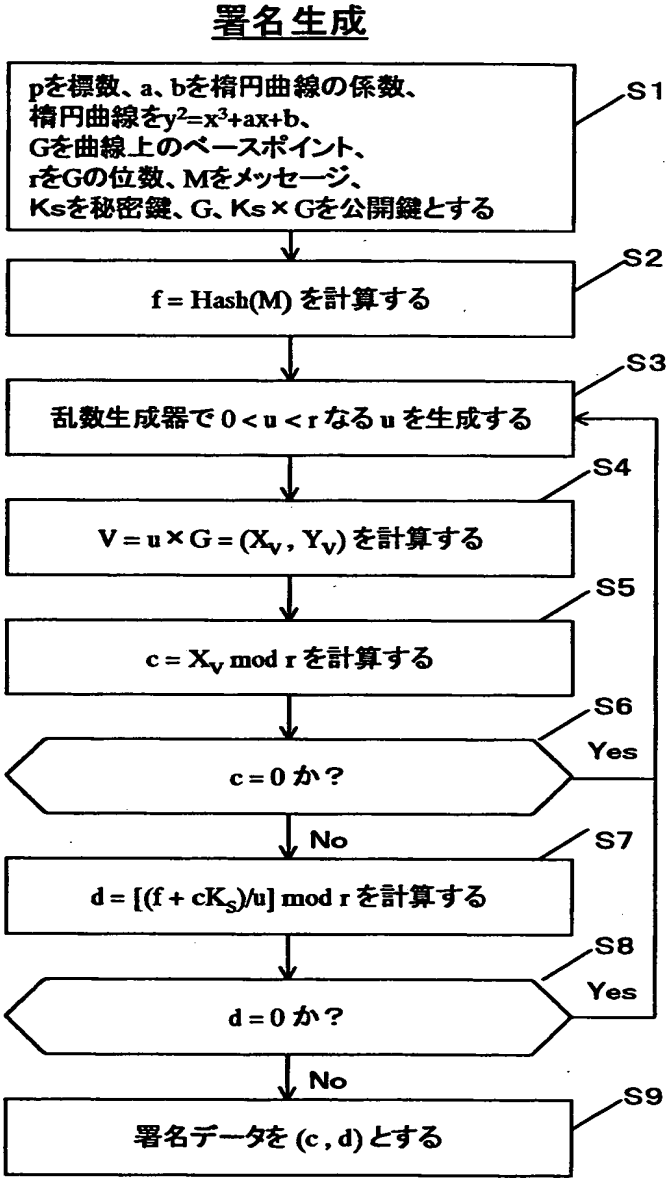
【図６】


発行ログ
発行情報
・発行金額
・ユーザデバイスID
・(ユーザID)
・有効期限
・シリアル番号
(クリアリングセンタ)
クリアリングセンタの署名
利用ログ
発行ログ
利用情報
・残高(オプション)
・利用金額
・受取先(to)
・利用サービス
(オプション)
・シリアル番号
(ユーザデバイス)
ユーザデバイスの署名
受領ログ
利用ログ
受領情報
・支払元(from)
・受領日時
・シリアル番号
(サービス
プロバイダ)
サービスプロバイダの署名
ユーザデバイスの署名
(ユーザ間の取引の場合)

【図７】

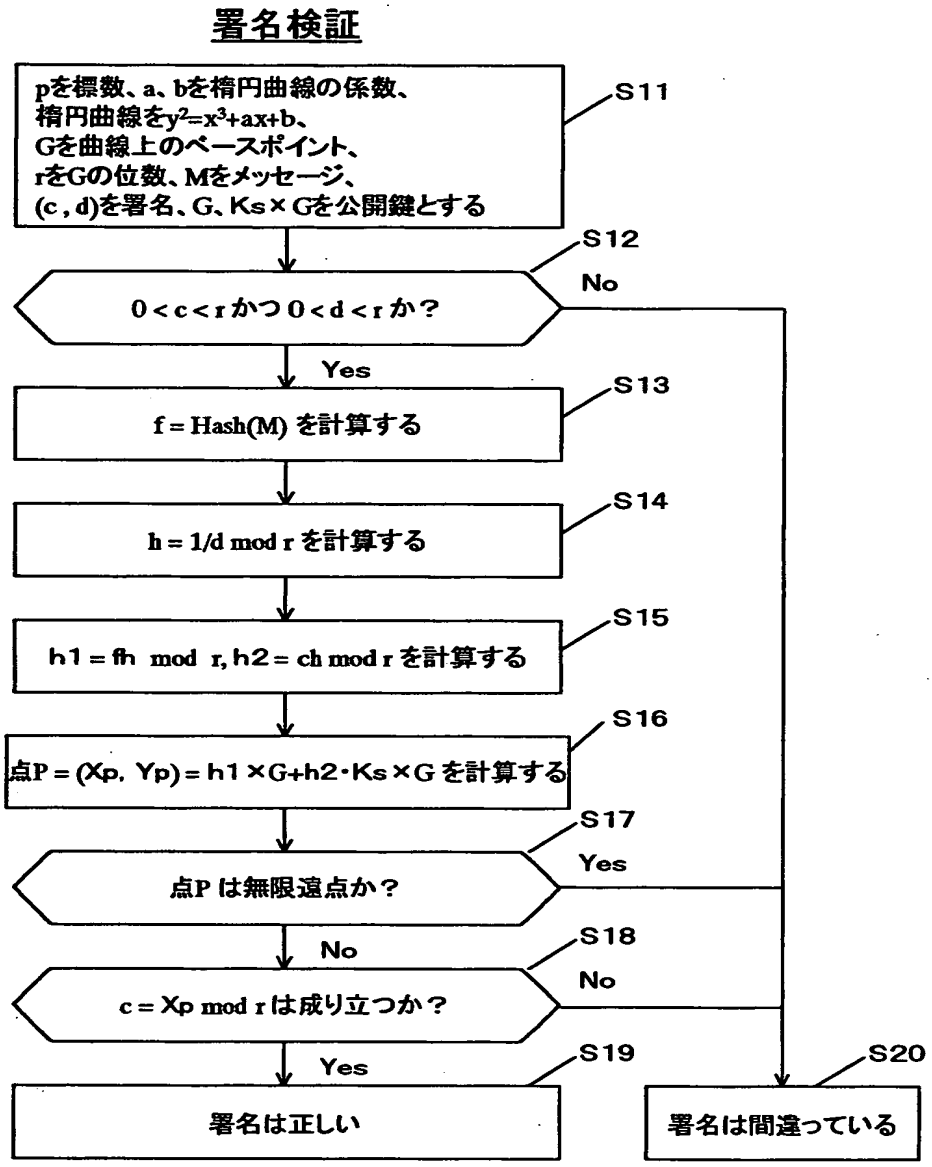

メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value: IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
En
メッセージ認証符号
(Message Authentication Code: MAC)
⊕ :排他的論理和処理(8バイト単位)

【図８】



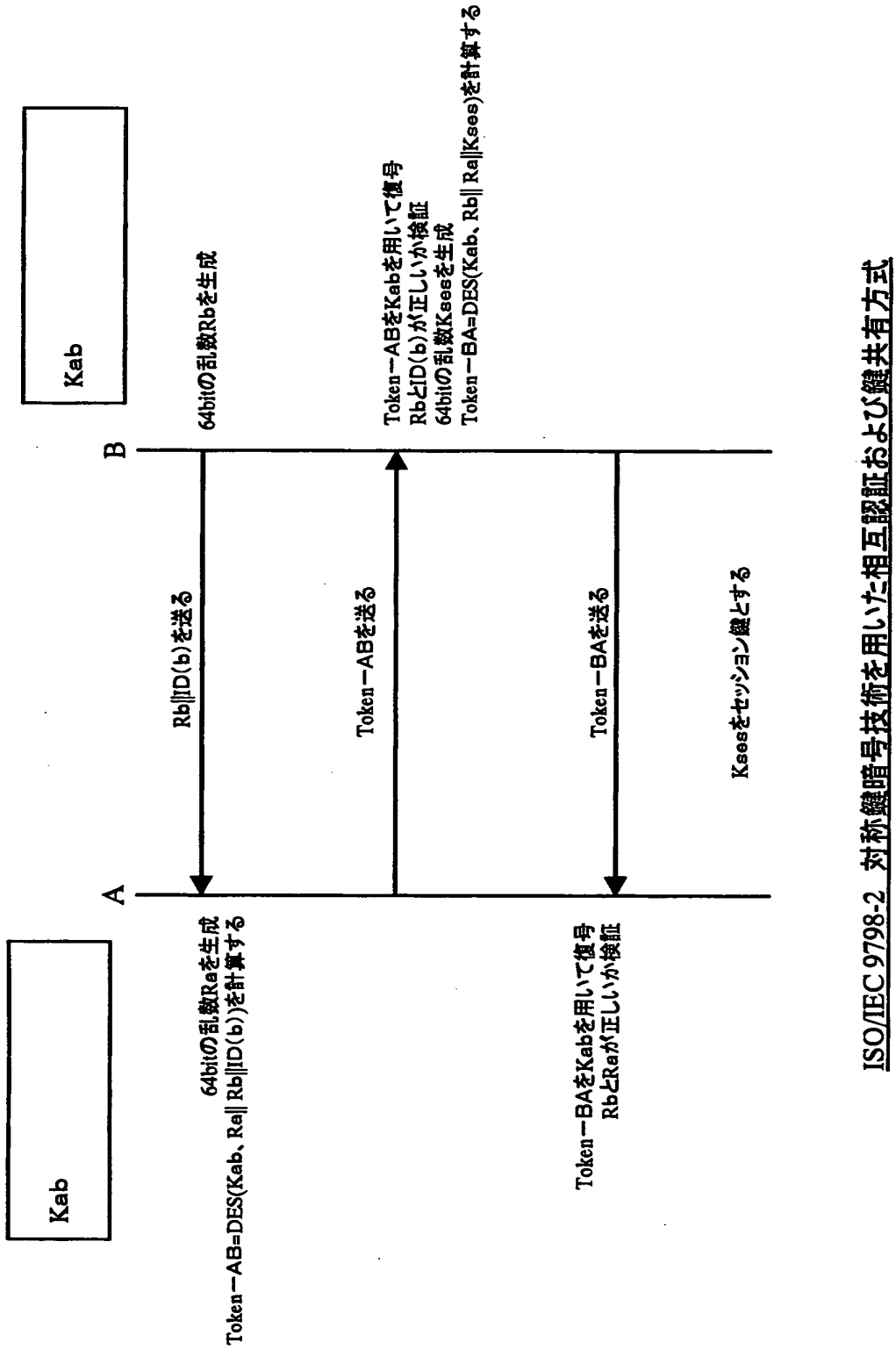
署名生成(IEEE P1363/D3)

【図９】



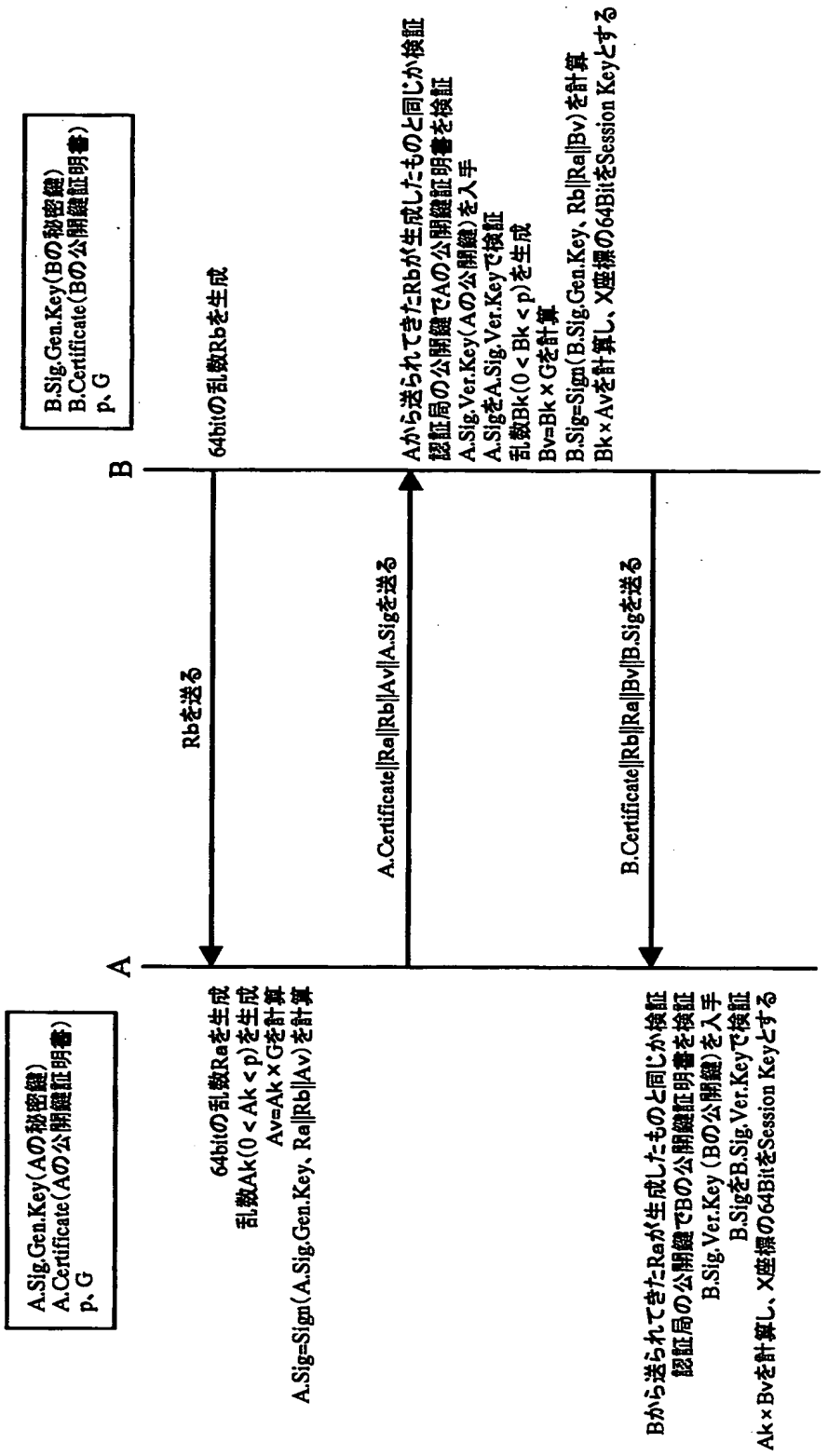
署名検証(IEEE P1363/D3)

【図１０】



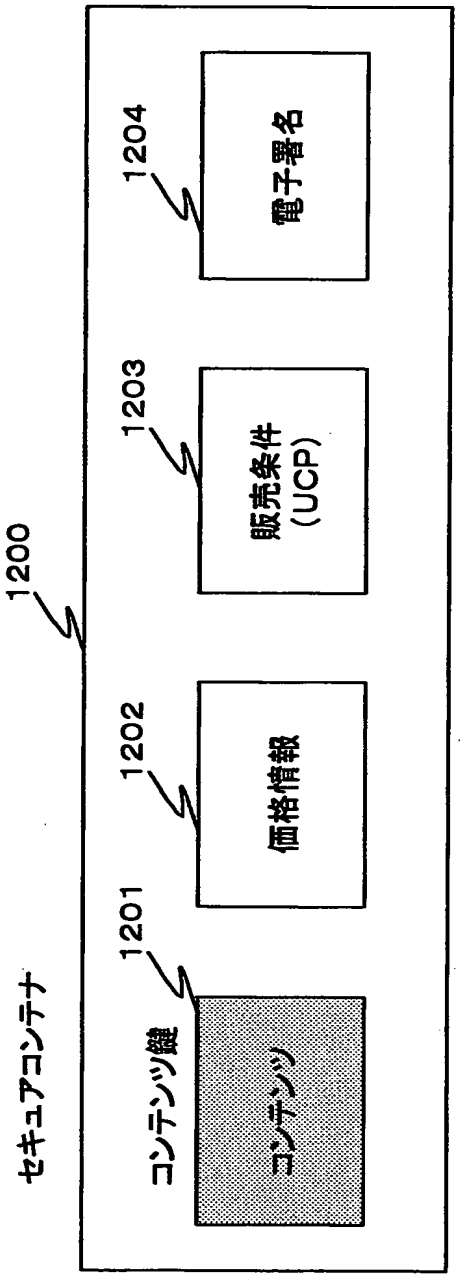
ISO/IEC 9798-2　対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１１】

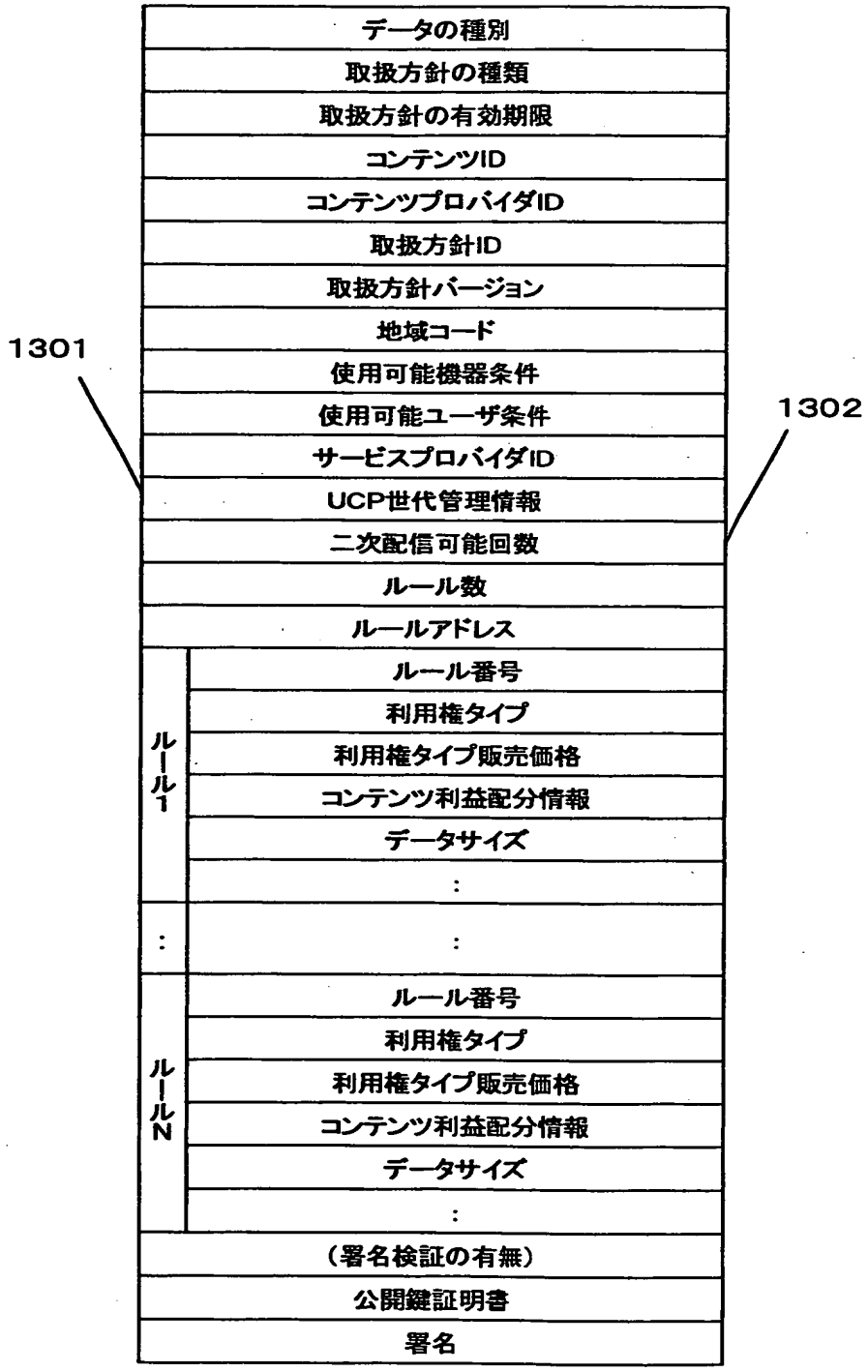


ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１２】


1200
セキュアコンテナ
1201
コンテンツ鍵
コンテンツ
1202
価格情報
1203
販売条件
(UCP)
1204
電子署名

【図１３】



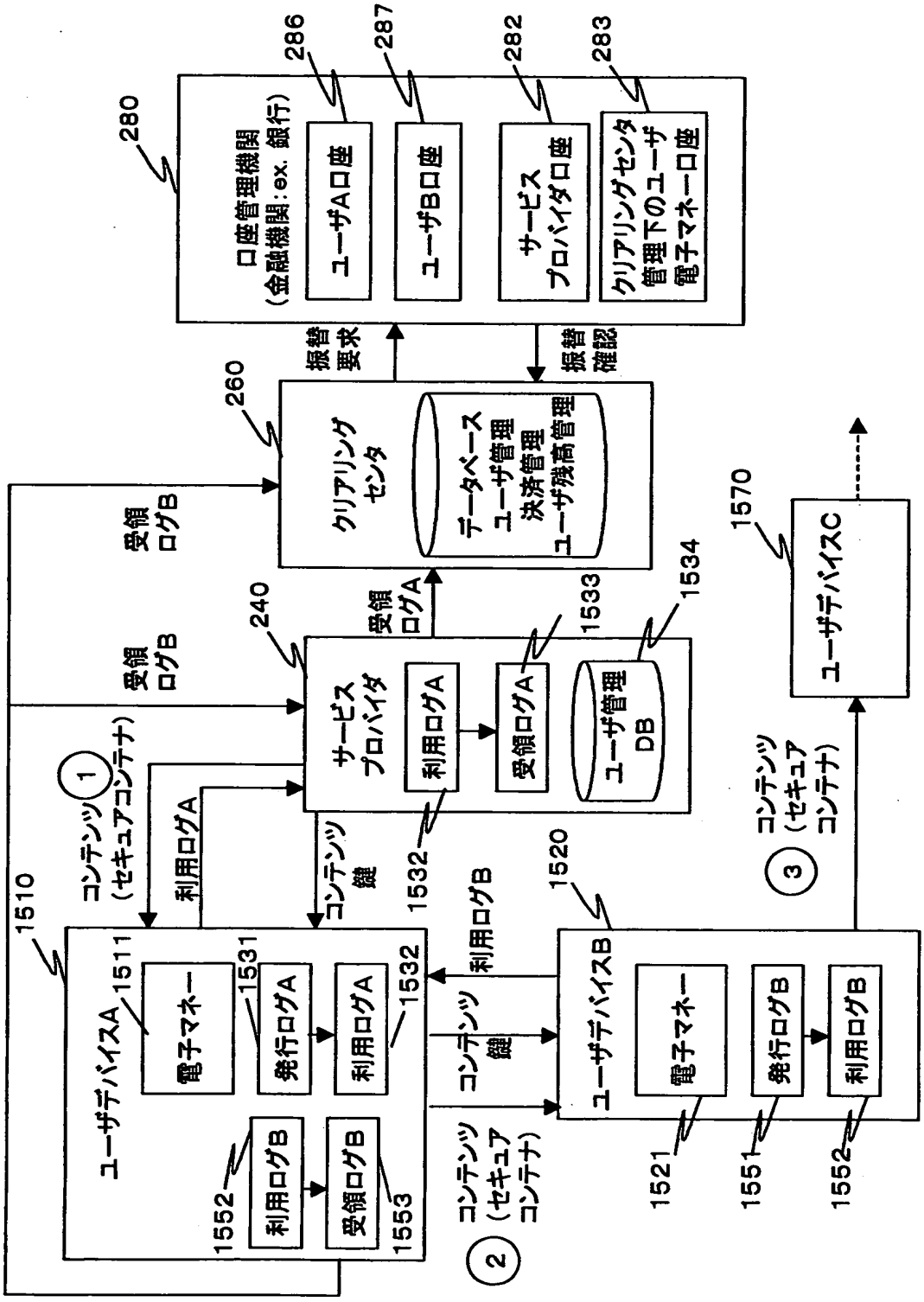
UCP(販売条件情報)

【図１４】

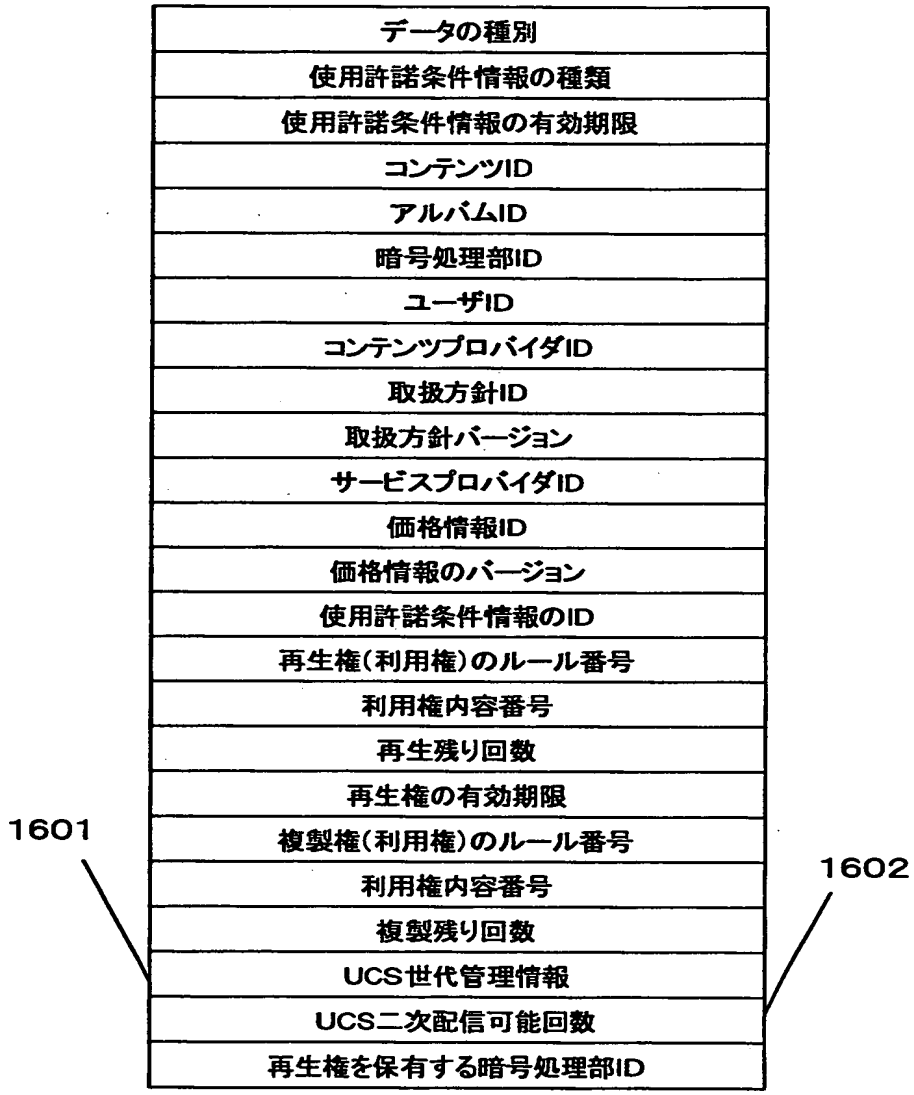
データの種別	
価格情報の種類	
価格情報の有効期限	
コンテンツID	
サービスプロバイダID	
価格情報ID	
価格情報バージョン	
地域コード	
使用可能機器条件	
使用可能ユーザ条件	
コンテンツプロバイダID	
取扱方針ID	
ルール数	
ルールアドレス	
ルール1	ルール番号
	コンテンツ利益配分情報
	価格
	データサイズ
	:
:	:
ルールN	ルール番号
	コンテンツ利益配分情報
	価格
	データサイズ
	:
（署名検証の有無）	
公開鍵証明書	
署名	

価格情報

【図１５】

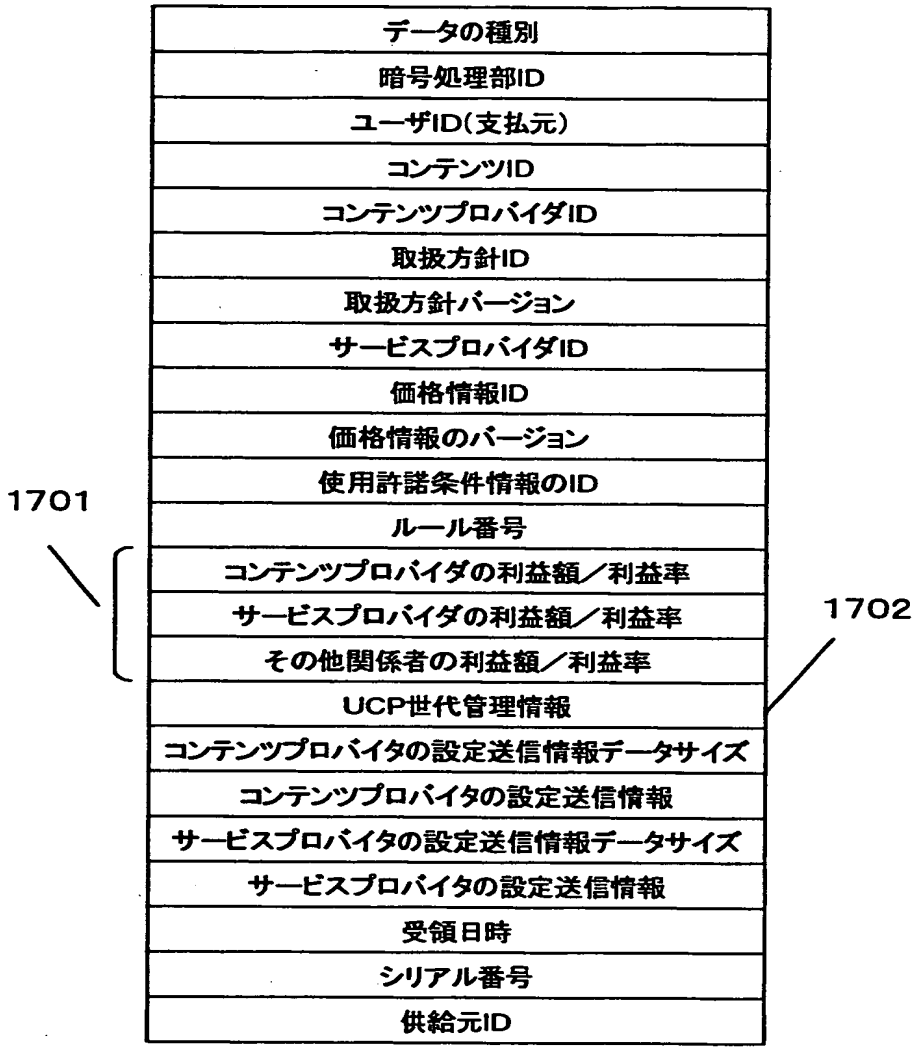

280
口座管理機関
（金融機関：ex. 銀行）
286
ユーザA口座
287
ユーザB口座
282
サービス
プロバイダ口座
283
クリアリングセンタ
管理下のユーザ
電子マネー口座
振替
要求
振替
確認
260
クリアリング
センタ
データベース
ユーザ管理
決済管理
ユーザ残高管理
受領
ログB
受領
ログB
受領
ログA
240
サービス
プロバイダ
利用ログA
受領ログA
1533
ユーザ管理
DB
1534
1570
ユーザデバイスC
コンテンツ
（セキュア
コンテナ）
①
利用ログA
コンテンツ
鍵
1532
1520
利用ログB
1510
ユーザデバイスA
1511
電子マネー
1531
発行ログA
利用ログA
1532
コンテンツ
鍵
ユーザデバイスB
電子マネー
発行ログB
利用ログB
1552
利用ログB
受領ログB
1553
コンテンツ
（セキュア
コンテナ）
②
1521
1551
1552
コンテンツ
（セキュア
コンテナ）
③

【図１６】



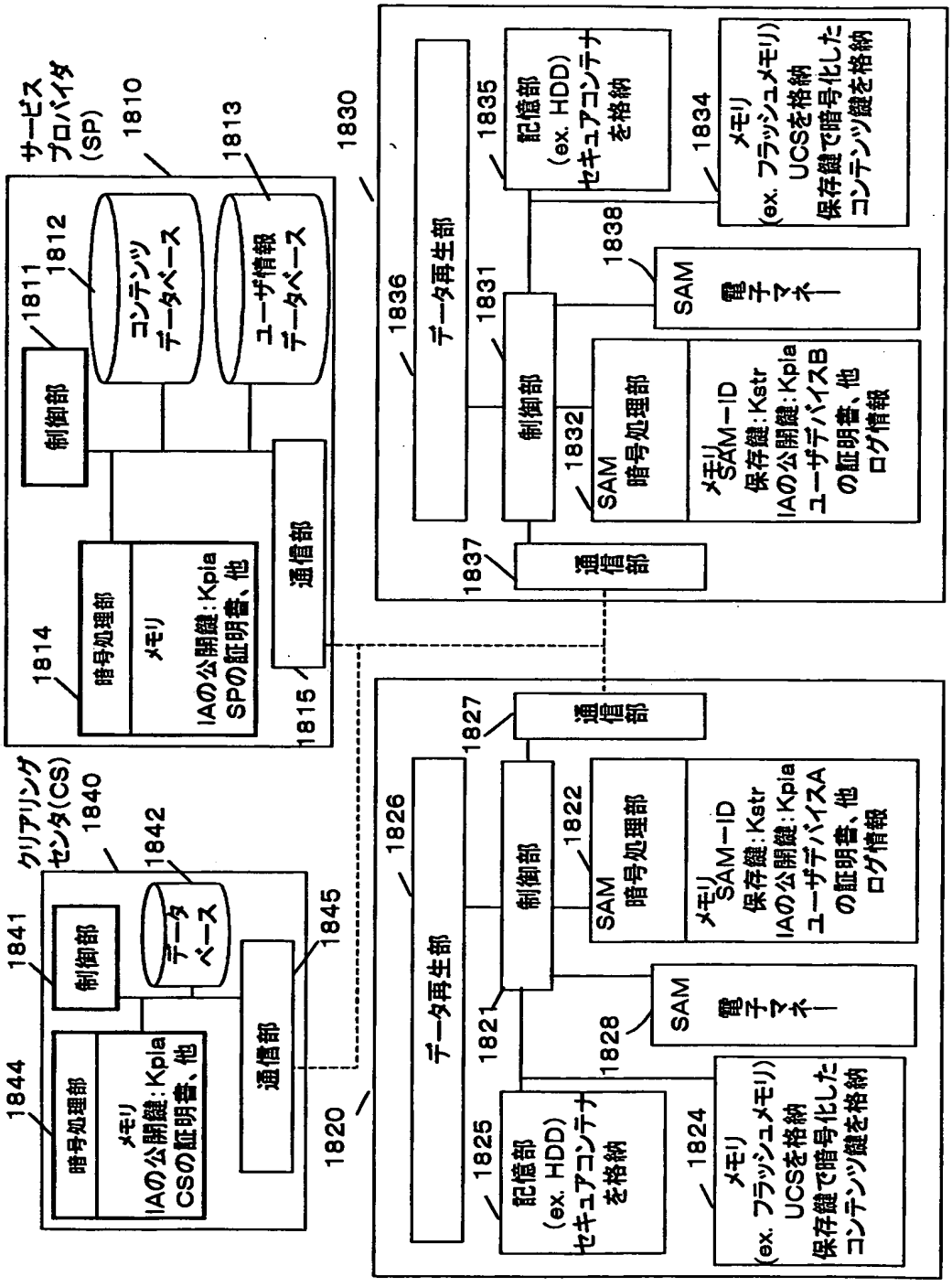
UCS(使用制御情報)

【図１７】

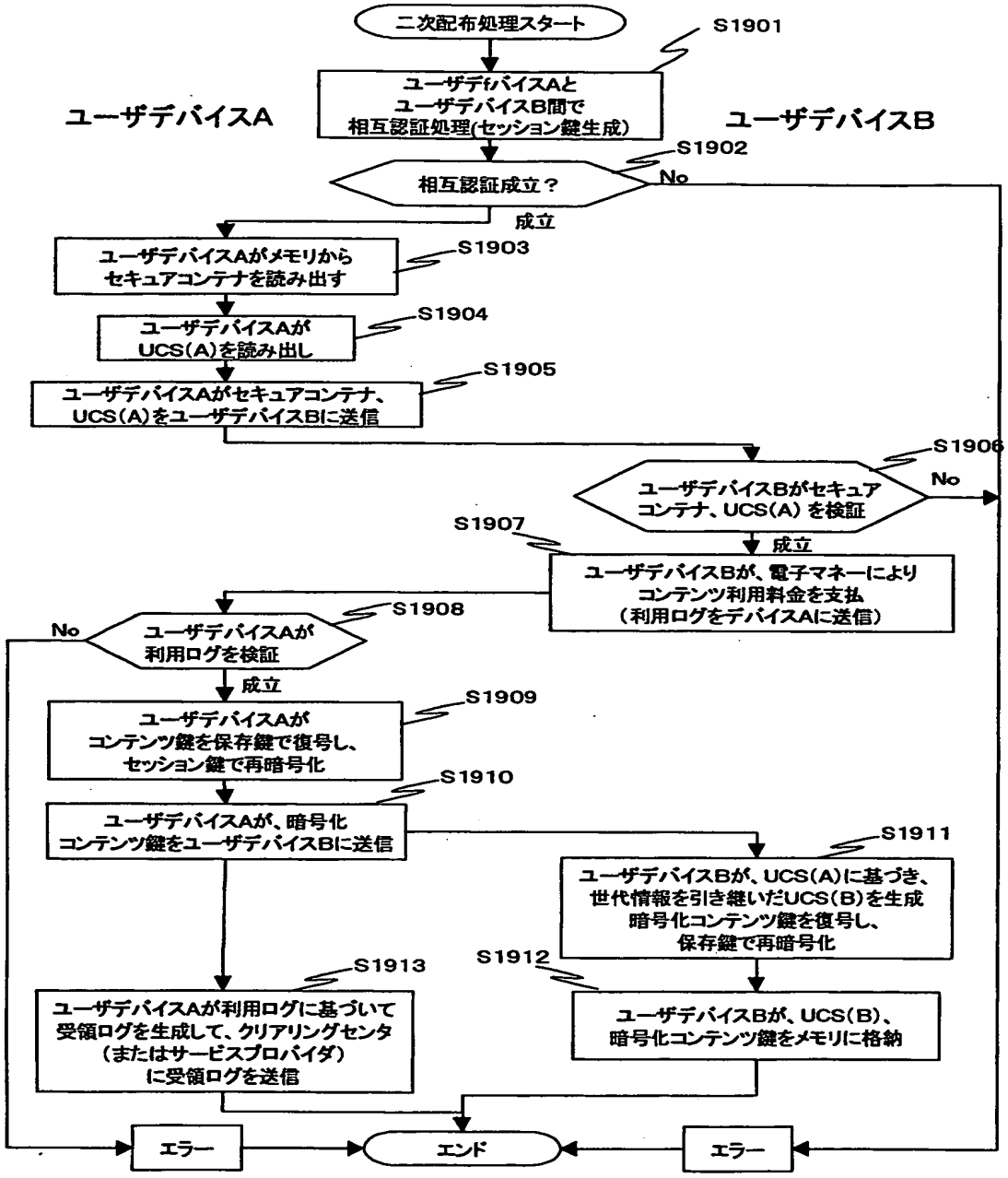

データの種別
暗号処理部ID
ユーザID(支払元)
コンテンツID
コンテンツプロバイダID
取扱方針ID
取扱方針バージョン
サービスプロバイダID
価格情報ID
価格情報のバージョン
使用許諾条件情報のID
ルール番号
コンテンツプロバイダの利益額／利益率
サービスプロバイダの利益額／利益率
その他関係者の利益額／利益率
UCP世代管理情報
コンテンツプロバイタの設定送信情報データサイズ
コンテンツプロバイタの設定送信情報
サービスプロバイタの設定送信情報データサイズ
サービスプロバイタの設定送信情報
受領日時
シリアル番号
供給元ID
1701
1702

受領情報

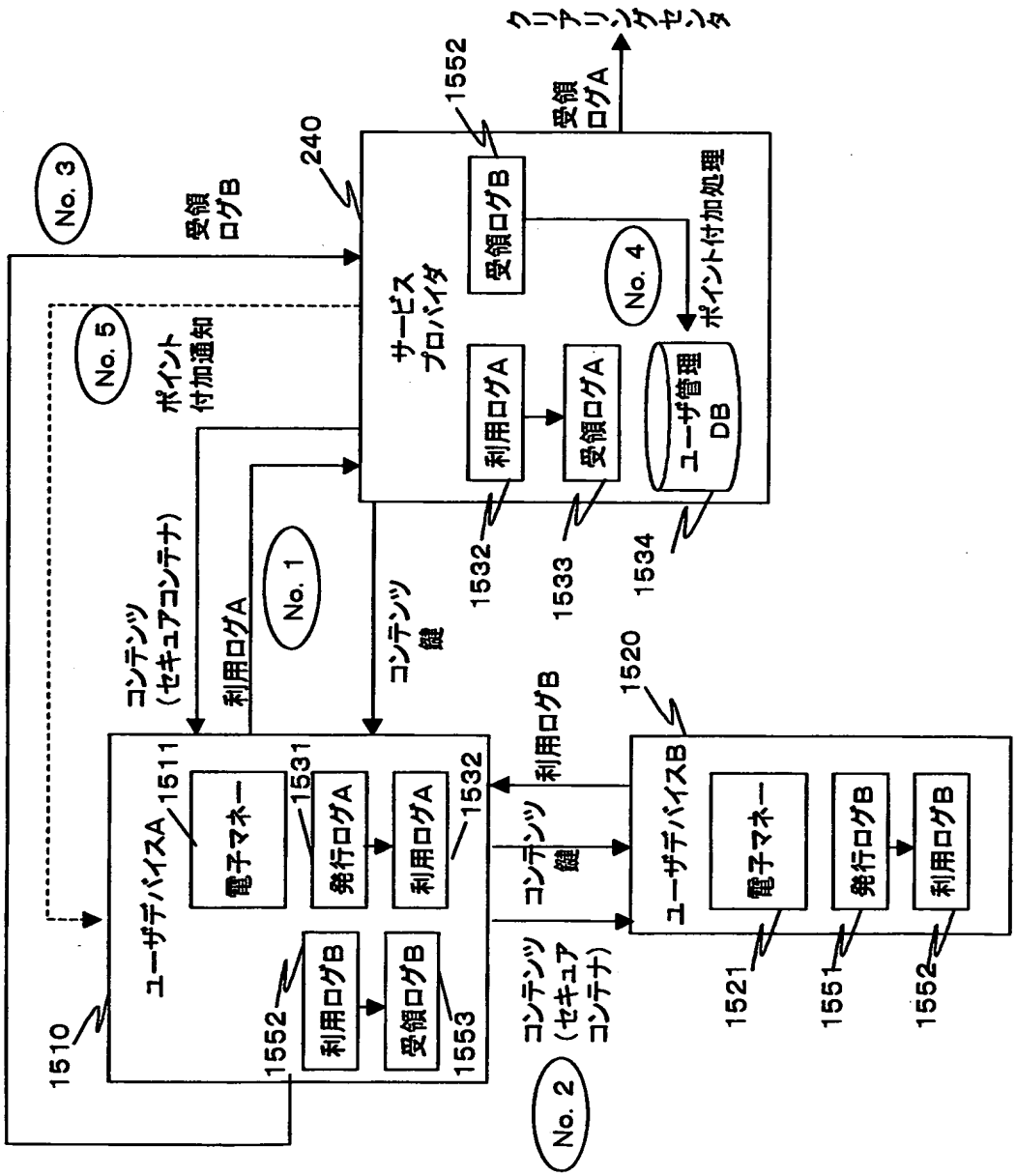
【図１８】


サービス
プロバイダ
(SP)
1810
1813
1830
1812
1811
コンテンツ
データベース
ユーザ情報
データベース
制御部
暗号処理部
メモリ
IAの公開鍵:Kpia
SPの証明書、他
通信部
1814
1815
クリアリング
センタ(CS)
1840
1842
1841
制御部
データ
ベース
暗号処理部
メモリ
IAの公開鍵:Kpia
CSの証明書、他
通信部
1844
1845
1820
データ再生部
1836
1831
制御部
1832
SAM
暗号処理部
メモリ
SAM−ID
保存鍵:Kstr
IAの公開鍵:Kpia
ユーザデバイスB
の証明書、他
ログ情報
SAM
電子マネー
1838
1834
メモリ
(ex. フラッシュメモリ)
UCSを格納
保存鍵で暗号化した
コンテンツ鍵を格納
1835
記憶部
(ex. HDD)
セキュアコンテナ
を格納
1837
通信部
ユーザデバイスB
1826
1821
1822
1827
通信部
データ再生部
制御部
SAM
暗号処理部
メモリ
SAM−ID
保存鍵:Kstr
IAの公開鍵:Kpia
ユーザデバイスA
の証明書、他
ログ情報
SAM
電子マネー
1828
1824
メモリ
(ex. フラッシュメモリ)
UCSを格納
保存鍵で暗号化した
コンテンツ鍵を格納
1825
記憶部
(ex. HDD)
セキュアコンテナ
を格納
ユーザデバイスA

【図１９】


二次配布処理スタート
S1901
ユーザデバイスA
ユーザデバイスAと
ユーザデバイスB間で
相互認証処理(セッション鍵生成)
ユーザデバイスB
S1902
相互認証成立？
No
成立
ユーザデバイスAがメモリから
セキュアコンテナを読み出す
S1903
ユーザデバイスAが
UCS(A)を読み出し
S1904
ユーザデバイスAがセキュアコンテナ、
UCS(A)をユーザデバイスBに送信
S1905
S1906
ユーザデバイスBがセキュア
コンテナ、UCS(A) を検証
No
S1907
成立
ユーザデバイスBが、電子マネーにより
コンテンツ利用料金を支払
（利用ログをデバイスAに送信）
S1908
No
ユーザデバイスAが
利用ログを検証
成立
S1909
ユーザデバイスAが
コンテンツ鍵を保存鍵で復号し、
セッション鍵で再暗号化
S1910
ユーザデバイスAが、暗号化
コンテンツ鍵をユーザデバイスBに送信
S1911
ユーザデバイスBが、UCS(A)に基づき、
世代情報を引き継いだUCS(B)を生成
暗号化コンテンツ鍵を復号し、
保存鍵で再暗号化
S1912
S1913
ユーザデバイスAが利用ログに基づいて
受領ログを生成して、クリアリングセンタ
（またはサービスプロバイダ）
に受領ログを送信
ユーザデバイスBが、UCS(B)、
暗号化コンテンツ鍵をメモリに格納
エラー
エンド
エラー

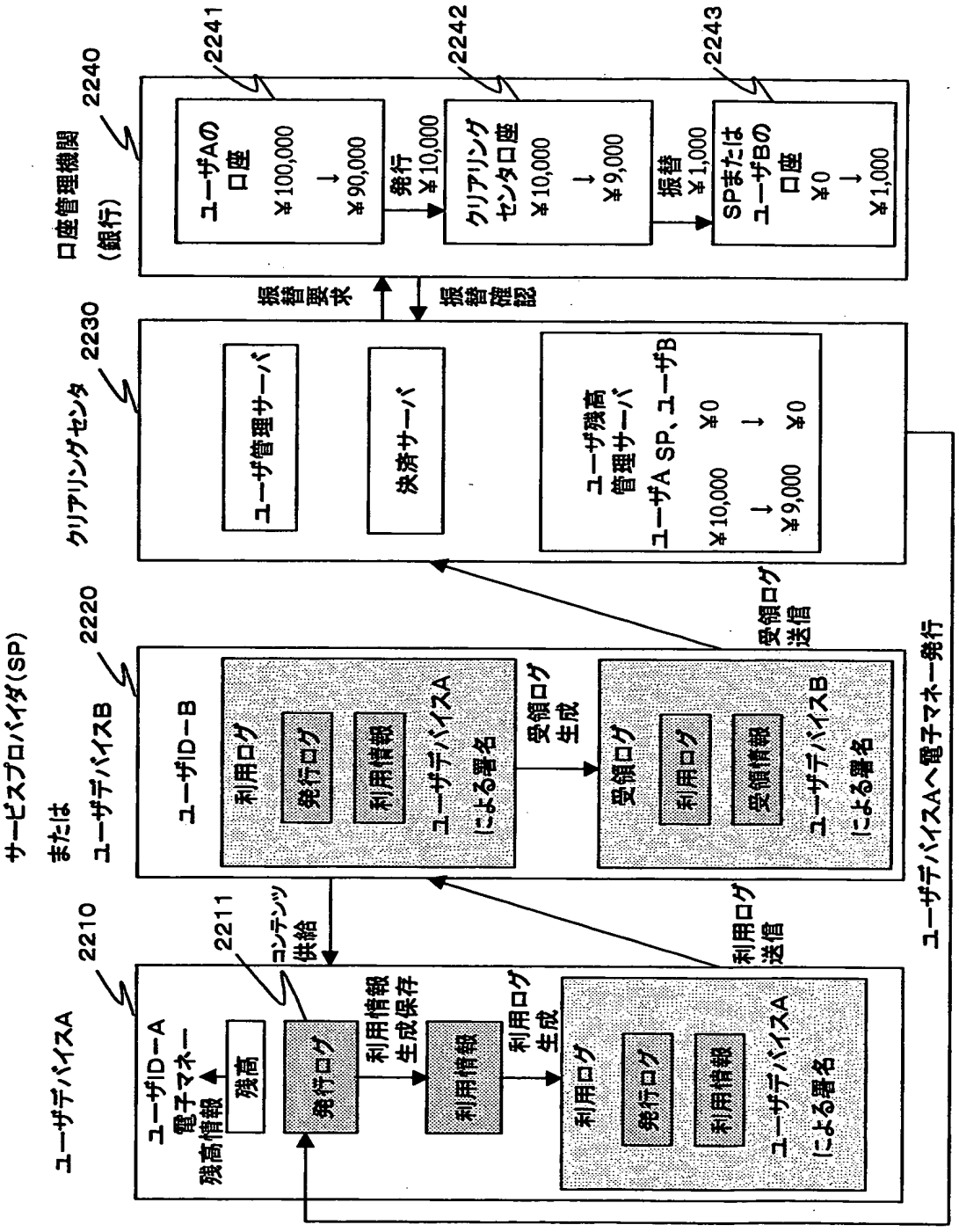
【図２０】


クリアリングセンタ
受領ログA
1552
240
No. 3
受領ログB
サービスプロバイダ
受領ログB
No. 4
ポイント付加処理
No. 5
ポイント付加通知
利用ログA
受領ログA
ユーザ管理DB
1532
1533
1534
コンテンツ（セキュアコンテナ）
利用ログA
No. 1
コンテンツ鍵
1520
利用ログB
ユーザデバイスA
1511
電子マネー
1531
発行ログA
利用ログA
1532
コンテンツ鍵
ユーザデバイスB
電子マネー
発行ログB
利用ログB
1510
1552
利用ログB
受領ログB
1553
コンテンツ（セキュアコンテナ）
No. 2
1521
1551
1552

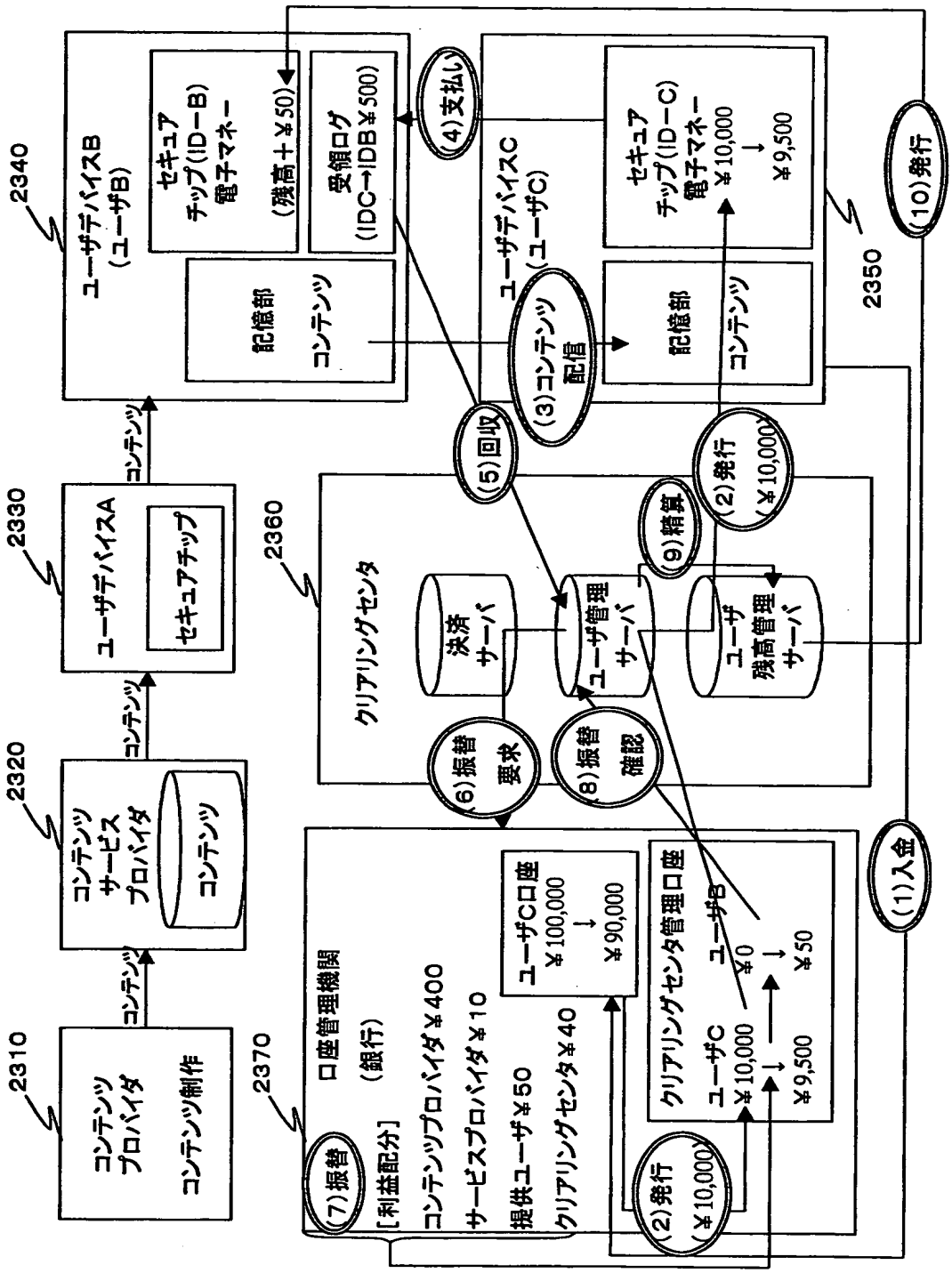
【図２１】

ユーザID	ユーザデバイスID	コンテンツID	受領ログID	ポイント
ABC0001	CDE00021	AAA001	BBB001	02
ABC0002	CDE00027	B05002	BA8822	05
ABC0003	CDE03211	CC0812	BA0214	12
：	：	：	：	：
BBC0231	EED02333	ABD325	BAA883	07

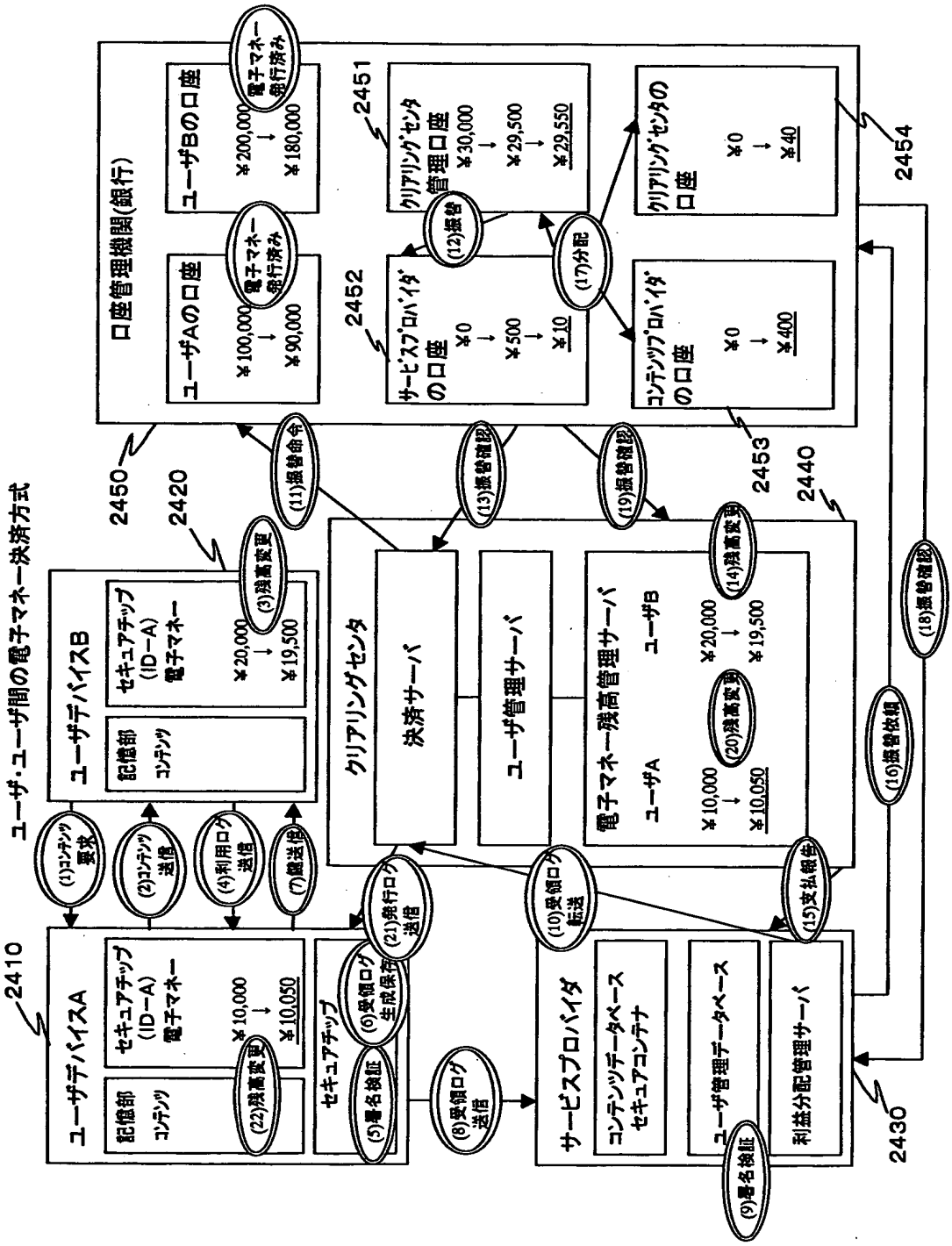
【図２２】


口座管理機関
(銀行)
2240
2241
2242
2243
ユーザAの
口座
¥100,000
→
¥90,000
発行
¥10,000
クリアリング
センタ口座
¥10,000
→
¥9,000
振替
¥1,000
SPまたは
ユーザBの
口座
¥0
→
¥1,000
振替要求
振替確認
クリアリングセンタ
2230
ユーザ管理サーバ
決済サーバ
ユーザ残高
管理サーバ
ユーザA SP、ユーザB
¥0
¥10,000
→
¥9,000
¥0
受領ログ
送信
サービスプロバイダ(SP)
または
ユーザデバイスB
2220
ユーザID－B
利用ログ
発行ログ
利用情報
ユーザデバイスA
による署名
受領ログ
生成
受領ログ
利用ログ
利用情報
ユーザデバイスB
による署名
コンテンツ
供給
2211
利用ログ
送信
ユーザデバイスA
2210
ユーザID－A
電子マネー
残高情報
残高
発行ログ
利用情報
生成保存
利用情報
利用ログ
生成
利用ログ
発行ログ
利用情報
ユーザデバイスA
による署名
ユーザデバイスへ電子マネー発行

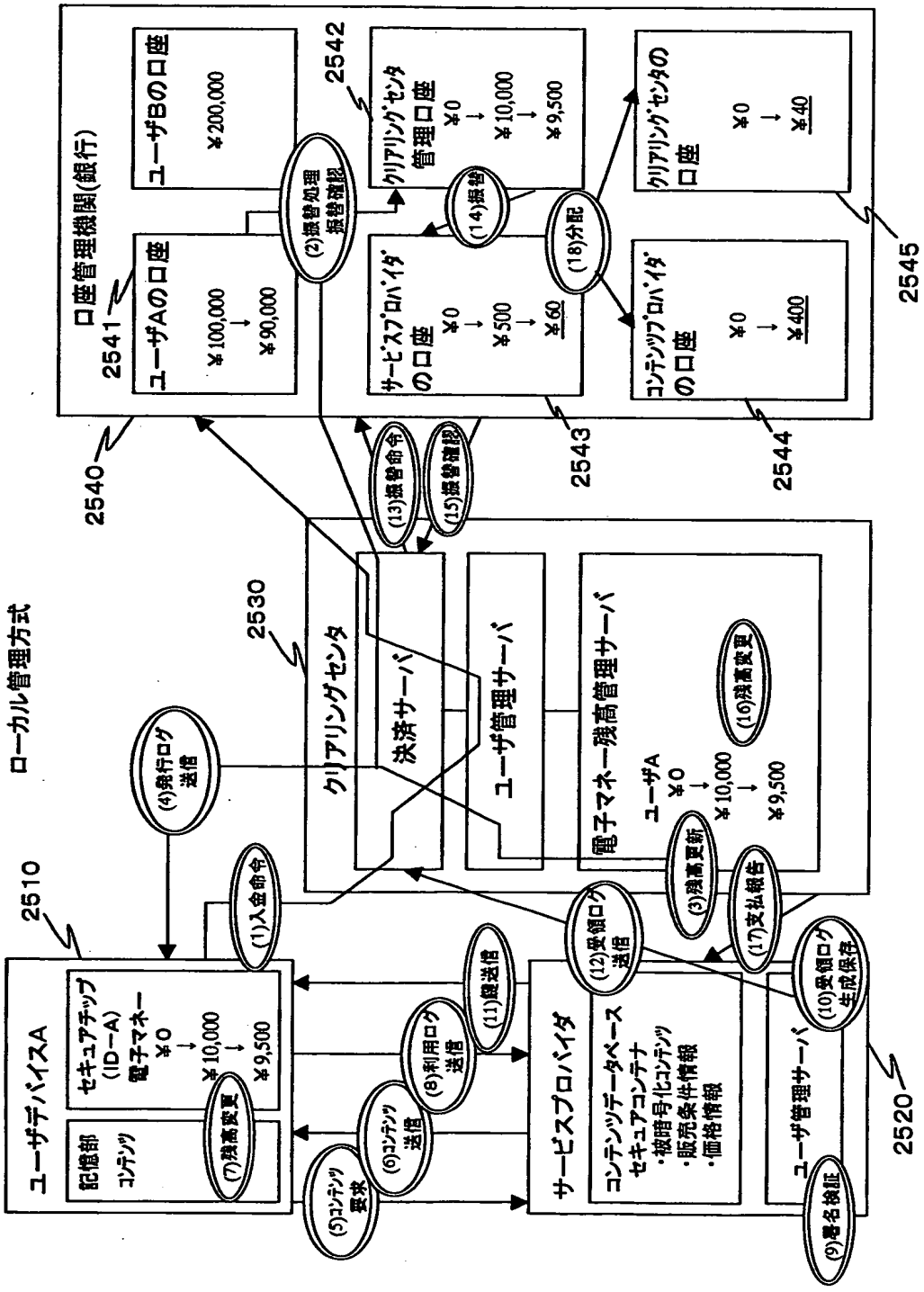
【図２３】


2310
コンテンツ
プロバイダ
コンテンツ制作
コンテンツ
2320
コンテンツ
サービス
プロバイダ
コンテンツ
コンテンツ
2330
ユーザデバイスA
セキュアチップ
コンテンツ
2340
ユーザデバイスB
(ユーザB)
セキュア
チップ(ID－B)
電子マネー－
(残高＋￥50)
受領ログ
(IDC→IDB￥500)
記憶部
コンテンツ
(4)支払い
ユーザデバイスC
(ユーザC)
セキュア
チップ(ID－C)
電子マネー－
￥10,000
→
￥9,500
記憶部
コンテンツ
2350
(10)発行
(3)コンテンツ
配信
(5)回収
2360
クリアリングセンタ
決済
サーバ
ユーザ管理
サーバ
ユーザ
残高管理
サーバ
(9)精算
(2)発行
(￥10,000)
(6)振替
要求
(8)振替
確認
2370
口座管理機関
(銀行)
[利益配分]
コンテンツプロバイダ￥400
サービスプロバイダ￥10
提供ユーザ￥50
クリアリングセンタ￥40
(7)振替
ユーザC口座
￥100,000
→
￥90,000
クリアリングセンタ管理口座
ユーザC
￥10,000
→
￥9,500
ユーザB
￥0
→
￥50
(2)発行
(￥10,000)
(1)入金

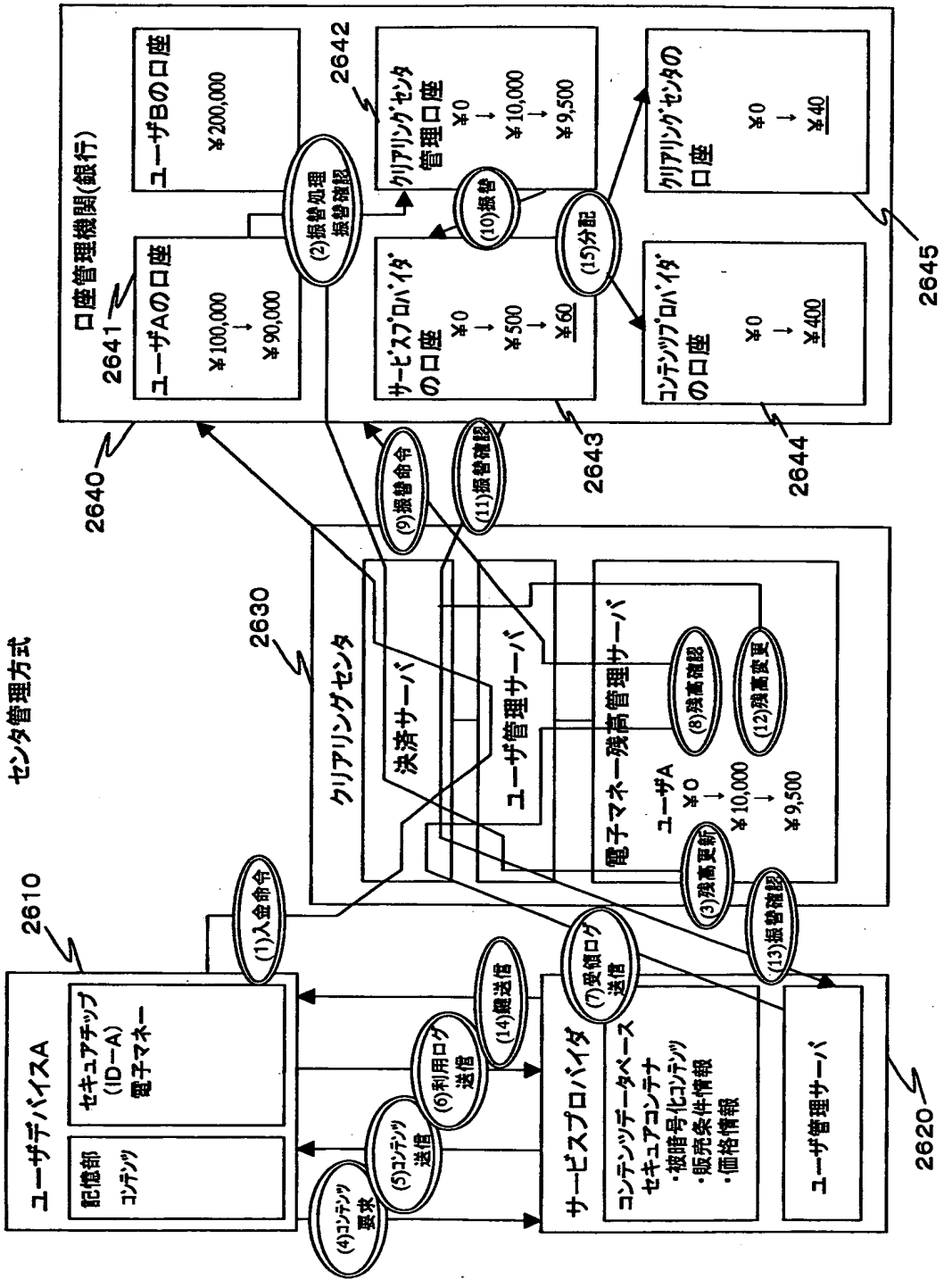
【図２４】


ユーザ・ユーザ間の電子マネー決済方式
口座管理機関(銀行)
ユーザAの口座
ユーザBの口座
サービスプロバイダの口座
クリアリングセンタ管理口座
コンテンツプロバイダの口座
クリアリングセンタの口座
2450
2451
2452
2453
2454
2410
2420
2430
2440
ユーザデバイスA
ユーザデバイスB
セキュアチップ
記憶部
コンテンツ
クリアリングセンタ
決済サーバ
ユーザ管理サーバ
電子マネー残高管理サーバ
サービスプロバイダ
コンテンツデータベース
ユーザ管理データベース
利益分配管理サーバ
(1)コンテンツ要求
(2)コンテンツ送信
(3)残高変更
(4)利用ログ送信
(5)署名検証
(6)受領ログ生成保存
(7)鍵送信
(8)受領ログ送信
(9)署名検証
(10)受領ログ転送
(11)振替命令
(12)振替
(13)振替確認
(14)残高変更
(15)支払報告
(16)振替依頼
(17)分配
(18)振替確認
(19)振替確認
(20)残高変更
(21)発行ログ送信
(22)残高変更
電子マネー発行済み
¥100,000 → ¥90,000
¥200,000 → ¥180,000
¥0 → ¥10 → ¥500
¥0 → ¥400
¥30,000 → ¥29,500 → ¥29,550
¥0 → ¥40
¥20,000 → ¥19,500
¥10,000 → ¥10,050
ユーザA
ユーザB

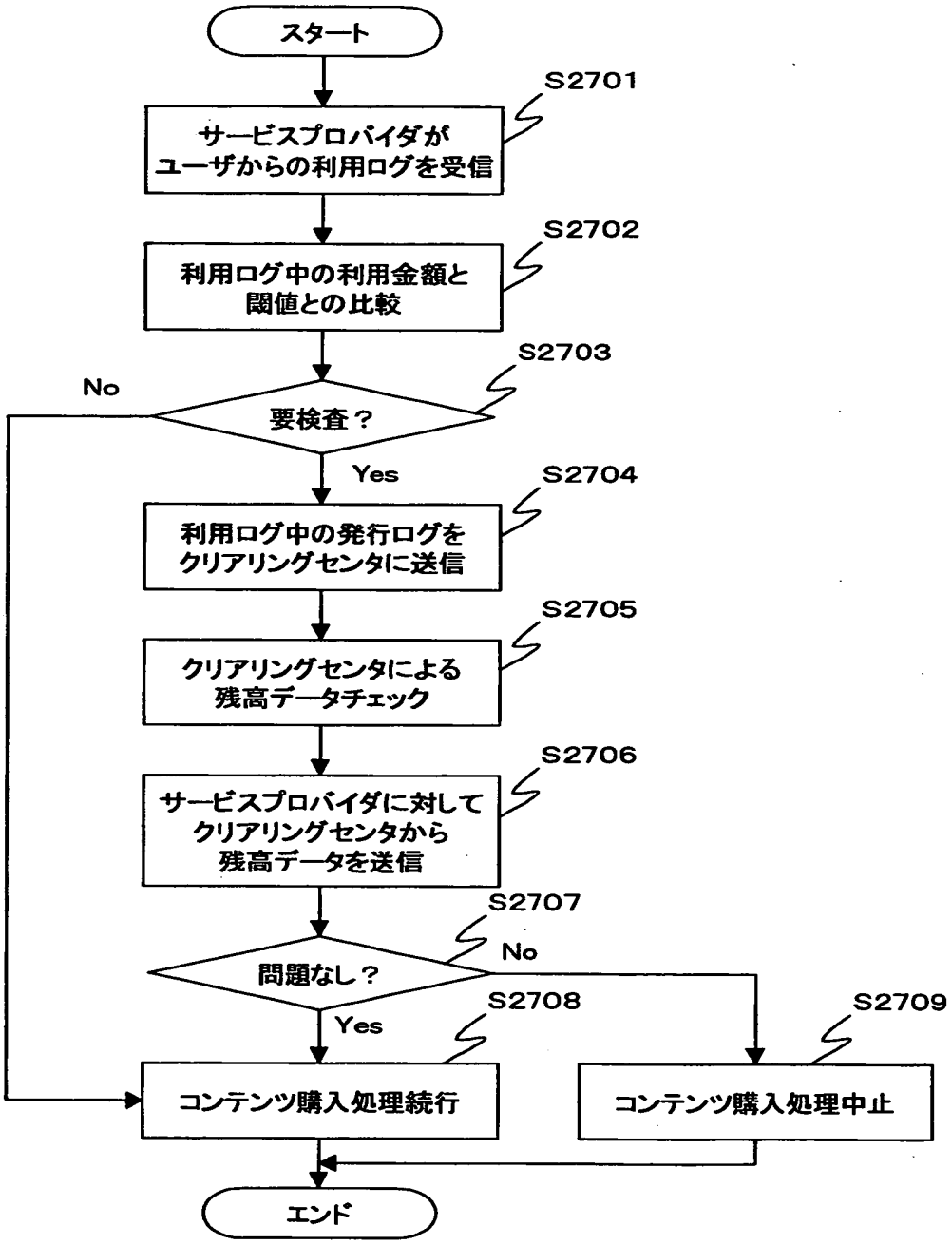
【図２５】


ローカル管理方式
2510
ユーザデバイスA
記憶部
コンテンツ
セキュアチップ
(ID−A)
電子マネー
¥0
→
¥10,000
→
¥9,500
(1)入金命令
(4)執行ログ送信
(7)残高変更
(5)コンテンツ要求
(6)コンテンツ送信
(8)利用ログ送信
(11)鍵送信
2530
クリアリングセンタ
決済サーバ
ユーザ管理サーバ
電子マネー残高管理サーバ
ユーザA
¥0
→
¥10,000
→
¥9,500
(3)残高更新
(16)残高変更
(17)支払報告
(12)受領ログ送信
(10)受領ログ生成依頼
(9)署名検証
2520
サービスプロバイダ
コンテンツデータベース
セキュアコンテナ
・被暗号化コンテンツ
・販売条件情報
・価格情報
ユーザ管理サーバ
2540
口座管理機関(銀行)
2541
ユーザAの口座
¥100,000
→
¥90,000
ユーザBの口座
¥200,000
(2)振替処理
振替確認
2542
クリアリング'センタ
管理口座
¥0
→
¥10,000
→
¥9,500
(14)振替
2543
サービスプロバイダ
の口座
¥0
→
¥500
→
¥60
(18)分配
2544
コンテンツプロバイダ
の口座
¥0
→
¥400
2545
クリアリング'センタの
口座
¥0
→
¥40
(13)振替命令
(15)振替確認

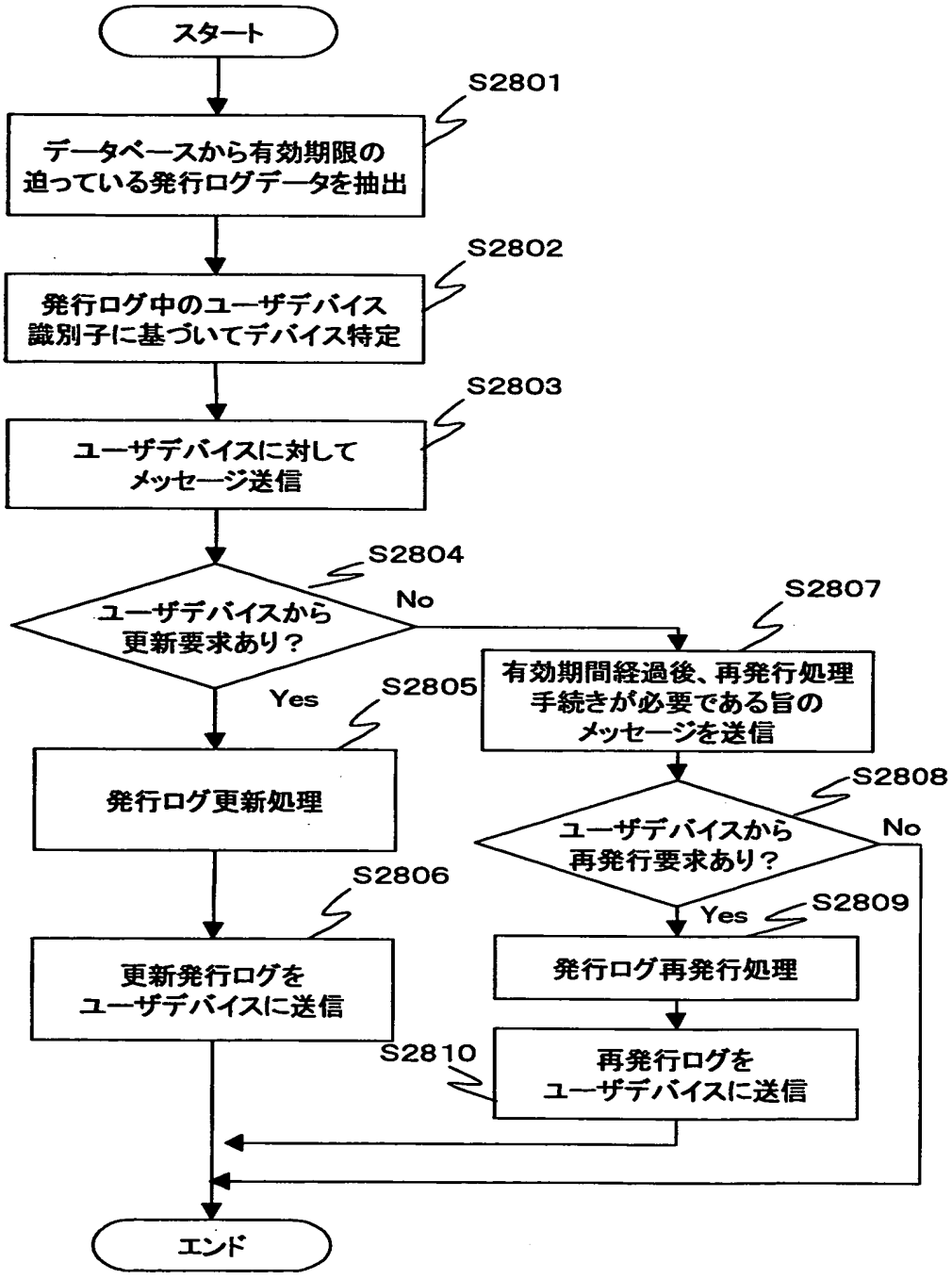
【図２６】


センタ管理方式
2610
ユーザデバイスA
セキュアチップ
(ID−A)
電子マネー
記憶部
コンテンツ
(1)入金命令
(4)コンテンツ
要求
(5)コンテンツ
送信
(6)利用ログ
送信
(14)鍵送信
2620
サービスプロバイダ
コンテンツデータベース
セキュアコンテナ
・被暗号化コンテンツ
・販売条件情報
・価格情報
(7)受領ログ
送信
ユーザ管理サーバ
2630
クリアリングセンタ
決済サーバ
ユーザ管理サーバ
電子マネー残高管理サーバ
ユーザA
¥0
→
¥10,000
→
¥9,500
(3)残高更新
(8)残高確認
(12)残高変更
(13)振替確認
(9)振替命令
(11)振替確認
2640
口座管理機関(銀行)
2641
ユーザAの口座
¥100,000
→
¥90,000
ユーザBの口座
¥200,000
(2)振替処理
振替確認
2642
クリアリング'センタ
管理口座
¥0
→
¥10,000
→
¥9,500
(10)振替
2643
サービスプロバイダ
の口座
¥0
→
¥500
→
¥60
(15)分配
2644
コンテンツプロバイダ
の口座
¥0
→
¥400
クリアリング'センタの
口座
¥0
→
¥40
2645

【図２７】


スタート
S2701
サービスプロバイダが
ユーザからの利用ログを受信
S2702
利用ログ中の利用金額と
閾値との比較
S2703
No
要検査？
Yes
S2704
利用ログ中の発行ログを
クリアリングセンタに送信
S2705
クリアリングセンタによる
残高データチェック
S2706
サービスプロバイダに対して
クリアリングセンタから
残高データを送信
S2707
No
問題なし？
Yes
S2708
S2709
コンテンツ購入処理続行
コンテンツ購入処理中止
エンド

【図２８】


スタート
S2801
データベースから有効期限の迫っている発行ログデータを抽出
S2802
発行ログ中のユーザデバイス識別子に基づいてデバイス特定
S2803
ユーザデバイスに対してメッセージ送信
S2804
ユーザデバイスから更新要求あり？
No
Yes
S2805
発行ログ更新処理
S2806
更新発行ログをユーザデバイスに送信
S2807
有効期間経過後、再発行処理手続きが必要である旨のメッセージを送信
S2808
ユーザデバイスから再発行要求あり？
No
Yes
S2809
発行ログ再発行処理
S2810
再発行ログをユーザデバイスに送信
エンド

【書類名】　要約書

【要約】

【課題】　コンテンツの決済処理を簡易にかつ確実に実行するコンテンツ取り引きシステムおよびコンテンツ取り引き方法を提供する。

【解決手段】　コンテンツを受領したユーザデバイスがコンテンツ販売条件に基づいて発行ログの発行金額を限度としたコンテンツ料金を電子マネーで支払い、コンテンツ識別子を含む利用ログを生成してサービスプロバイダに送信する。サービスプロバイダは利用ログに基づいて受領ログを生成してクリアリングセンタに送信する。クリアリングセンタは、受領ログに基づいて電子マネーの精算処理を実行し振替処理要求を口座管理機関に送信する。これら一連の処理を暗号データ送信により実行することでコンテンツ利用料の精算が安全に処理される。

【選択図】　図４

出証特２０００－３１０９４６０

出 願 人 履 歴 情 報

識別番号　〔０００００２１８５〕

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社